Valparaiso University Law Review

Volume 45
Number 4 *Summer 2011*

*pp.*215-273

Summer 2011

No Requirement Left Behind: The Inadvertent Discovery Requirement—Protecting Citizens One File at a Time

Nicholas Hood

Note

NO REQUIREMENT LEFT BEHIND: THE INADVERTENT DISCOVERY REQUIREMENT—PROTECTING CITIZENS ONE FILE AT A TIME

I. INTRODUCTION

With the advent of computers came the dawn of a new age—a Digital Age. Many take for granted the ability of computers to assist and manage our daily lives, but few recognize that complex problems arise through the application of historic doctrines to new technology.[1] For instance, during the government investigation of steroid use in Major League Baseball, government officials obtained a search warrant to seize the steroid testing results of ten specific players.[2] However, in executing

---

[1] Perhaps Justice Stewart said it best almost forty years ago when he aptly cautioned that "[i]f times have changed . . . in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important." Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971).

[2] United States v. Comprehensive Drug Testing, Inc. (*Comprehensive Drug Testing III*), 579 F.3d 989, 993 (9th Cir. 2009) (en banc), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc). Although the Ninth Circuit revised its decision, the only substantial change was the omission of certain language affirmatively implementing mandatory government procedures, which instead now comprises part of a concurring opinion. *See* United States v. Comprehensive Drug Testing, Inc. (*Comprehensive Drug Testing IV*), 621 F.3d 1162, 1165 (9th Cir. 2010) (en banc); *id.* at 1178 (Kozinski, C.J., concurring). For this reason, citations hereinafter to the *Comprehensive Drug Testing* decision will reference both en banc panel decisions, and will do so interchangeably at times (although the Notewriter is aware the original en banc decision was ultimately revised and superseded).

This decision has an extensive procedural history. The case was first decided in front of a panel of three Ninth Circuit judges, and the opinion can be found at *United States v. Comprehensive Drug Testing, Inc.* (*Comprehensive Drug Testing I*), 473 F.3d 915 (9th Cir. 2006). This panel decision was withdrawn and superseded by a second panel decision also consisting of three judges; the opinion can be found at *United States v. Comprehensive Drug Testing, Inc.* (*Comprehensive Drug Testing II*), 513 F.3d 1085 (9th Cir. 2008). This second panel decision was ultimately withdrawn, and the case was heard en banc before eleven judges of the Ninth Circuit. *See Comprehensive Drug Testing III*, 579 F.3d at 993.

Because of the potentially enormous impact of the decision, the Ninth Circuit, on November 4, 2009, ordered that both parties "file simultaneous briefs addressing whether this case should be reheard en banc by the full court" by November 25, 2009. Order for United States v. Comprehensive Drug Testing, Inc., No. 05-10067 (9th Cir. Nov. 4 2009), *available at* http://volokh.com/wp/wp-content/uploads/2009/11/CDTOrder.pdf. On November 23, 2009, the Department of Justice also filed an amicus brief in support of the rehearing en banc by the full court. Brief for the United States in Support of Rehearing En

the warrant, the officials gained access to test results of thousands of other professional athletes from various professional sports.[3] The difficult issue the United States Court of Appeals for the Ninth Circuit had to resolve was whether the government should be able to keep the information relating to the players not specified in the warrant.[4]

To date, only two Circuits—the Ninth and Tenth—have comprehensively addressed the unique issues raised by searches and seizures of computer-related or electronically stored information.[5] Furthermore, district courts have been unable to agree on a coherent understanding of how to reconcile new technology and existing standards.[6] As a result, the case law and commentary regarding the application of constitutional doctrines to the search and seizure of computer information is discordant.[7] At worst, there is high potential that courts will adopt misguided notions of constitutional protection and

---

Banc by the Full Court, *Comprehensive Drug Testing III*, 579 F.3d 989 (2009) (No. 05-10067). Subsequently, the Ninth Circuit heard the case again en banc, resulting in *Comprehensive Drug Testing IV*, 621 F.3d 1162.

[3] *Comprehensive Drug Testing III*, 579 F.3d at 993. The information seized by the government included, inter alia, the master list of all MLB players tested during the 2003 season and a list of positive drug test results for eight of the ten specified players, intermingled with positive results for twenty-six other MLB players. *Id*. at 997.

[4] *Id*. The Ninth Circuit described the case as being about "the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information." *Id*. at 993.

[5] *See infra* Part II.B.2–3 (discussing the Ninth and Tenth Circuit's approach to the issue); *infra* Part III.B–III.C (analyzing the positive and negative aspects of each approach). For the purposes of this Note, the terms "computer-related," "digital," "electronic," "electronically stored," and "magnetically stored" evidence refer to the same general category of evidence. This evidence is generally the same as the evidence described in the Federal Rules of Civil Procedure as "electronically stored information." *See* FED. R. CIV. P. 34(a) (Notes of Advisory Committee on 2006 Amendments) (noting that the wide variety of computer systems currently in use and the rapid pace of technological change counsels against a limiting or precise definition of electronically stored information). The Committee was wise in using a term that accounts for all current methods of computer information and still allows for technological advancements. *See id*. (indicating that the term electronically stored information should encompass data "stored in any medium" and allow for future developments in computer technology; it is a term "intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments").

[6] *See infra* Parts II–III (providing background and analysis of the different approaches that circuit and district courts have taken to resolve novel issues).

[7] *Compare Comprehensive Drug Testing III*, 579 F.3d at 998 (holding that the government should forswear use of the plain view doctrine in digital evidence cases), *with* United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) (holding that where police inadvertently discovered child pornography during search for fake ID-related information and subsequently applied for a second warrant, no constitutional violation occurred), *and* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that the subjective intent of the officer is determinative).

thereby compromise the privacy and possessory interests of all Americans. To ensure that the correct balance is struck between these two competing interests—the interest of the individual and that of the state—courts must espouse a solution that is sensitive to the efforts of law enforcement officials, while retaining the explicit protections provided by the Fourth Amendment of the Constitution.[8]

This Note will first briefly provide a historical context of the Fourth Amendment, presenting relevant background information, detailing its two main requirements, and defining the terms of art within its text.[9] Part II further examines existing jurisprudential theories and how they attempt to reconcile the plain view doctrine with electronically stored and computer-related evidence.[10] Next, Part III analyzes the feasibility of the various approaches and concludes that currently no one approach adequately balances all of the competing interests.[11] Finally, Part IV offers a solution to the problems created by computer-related evidence and proposes that the Supreme Court implement the inadvertent discovery requirement of *Coolidge v. New Hampshire* as applied to such evidence.[12]

II. BACKGROUND

Searches and seizures of computer data stored on personal computers and within extensive computer databases will compel courts to resolve situations in which relevant, incriminating evidence is intermingled with highly personal and entirely unrelated information. To date, at least one man has been sentenced to death following an officer's electronic recovery of incriminating notes that were previously

---

8 *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (**"**On one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order."); *Comprehensive Drug Testing III*, 579 F.3d at 1004 ("This case well illustrates both the challenges faced by modern law enforcement in retrieving information it needs to . . . prosecute wrongdoers, and the threat to the privacy of innocent parties from a vigorous criminal investigation.").

9 *See infra* Part II (presenting an overview of the history of the Fourth Amendment and what it has come to require).

10 *See infra* Part II (examining the existing avenues that courts have taken to reconcile the Fourth Amendment's requirements, the plain view doctrine, and searches for electronically stored evidence).

11 *See infra* Part III (analyzing the positive and negative aspects of varying approaches).

12 *See infra* Part IV (proposing that the Supreme Court preserve *Coolidge*'s inadvertent discovery requirement as applied to digital evidence by distinguishing such evidence from the physical evidence in *Horton v. California*, 496 U.S. 128, 137–38 (1990)).

deleted.[13] The government has also indicted a college student on felony fraud and software piracy charges after the government monitored the student's website postings.[14] This novel dilemma has yet to receive a great deal of attention from courts despite its inevitable significance on modern American life, and remains a relatively undeveloped area of Fourth Amendment jurisprudence.[15] However, two circuit courts addressed the issue—one directly and one indirectly—and formulated a special doctrine in an attempt to handle these searches and seizures.[16]

Part II.A of this Note provides a general background to the Fourth Amendment, including information about its history and the motivation for its drafting and ratification.[17] Next, Part II.A.1 and Part II.A.2 examine two of the most essential requirements in Fourth Amendment analysis: the warrant requirement and the particularity requirement, respectively.[18] Then, Part II.A.3 precisely addresses what the term "seizure" means within Fourth Amendment jurisprudence.[19] Next, Part II.B of this Note discusses the Fourth Amendment's application to computer evidence, the plain view doctrine (an exception to the warrant requirement), and the differing approaches that courts have taken in an attempt to solve the problem of applying the plain view doctrine in the context of computer-related evidence cases.[20]

---

13 *See* Commonwealth v. Copenhefer, 587 A.2d 1353, 1356–57 (Pa. 1991) (affirming appellant's murder conviction and death sentence and holding, inter alia, that appellant's attempt to delete computer files created only a mere hope of secrecy, which was not synonymous with a legally cognizable expectation of privacy).

14 Peter H. Lewis, *Student Accused of Running Network for Pirated Software*, N.Y. TIMES, Apr. 9, 1994, at A1 (discussing the government's monitoring of a college student's electronic bulletin board and Internet site, which ultimately resulted in a felony indictment on fraud and software piracy charges); *see also* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 77 n.11 (1994) (recounting these and many more horror stories involving overly broad searches and seizures of computer evidence).

15 *See, e.g.*, United States v. Jinwoo Kim, 677 F. Supp. 2d 930, 944 (S.D. Tex. 2009) (basing almost the entire opinion off of Ninth Circuit case law because "neither the Fifth Circuit nor the United States Supreme Court have developed precedent" and "the Ninth Circuit has the most robust body of law on the subject matter.").

16 *See infra* Part II.B.2–3 (providing a background of the Ninth and Tenth Circuit's differing approaches to the issue).

17 *See infra* Part II.A (discussing the history of the Fourth Amendment as well as general Fourth Amendment principles).

18 *See infra* Part II.A.1 (discussing the warrant requirement); *infra* Part II.A.2 (discussing the particularity requirement).

19 *See infra* Part II.A.3 (discussing the meaning of the term "seizure" within Fourth Amendment analysis).

20 *See infra* Part II.B (discussing the Fourth Amendment as applied to computers, the plain view doctrine, and the differing approaches courts utilize to reconcile the two).

A. The Requirements of the Fourth Amendment

The Fourth Amendment to the Constitution was adopted by Congress in 1789 and ratified by the states as a provision of the Bill of Rights in 1791.[21] The Fourth Amendment guards against unreasonable searches and seizures by both federal and local law enforcement officials.[22] It was drafted and ratified to ensure that the overly intrusive general searches conducted under English rule were not reinstated in the new nation.[23] When examining the Fourth Amendment, the interests at

---

[21] U.S. CONST. amend. IV; Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 724 (1999). *See generally* ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE pt. 1 (2006) (providing a descriptive account of early Fourth Amendment history and its surrounding circumstances).

[22] Elkins v. United States, 364 U.S. 206, 215 (1960). The Fourth Amendment ensures that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. Fourth Amendment history indicates that it was drafted to guard against the use of general warrants and Writs of Assistance, which were prevalent in Colonial England. 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.10 (4th ed. 2008) [hereinafter LAFAVE, SEARCH AND SEIZURE]. The drafters of the Constitution considered such broad searches to be an unreasonable intrusion of privacy that necessitated protection. *Id*. The Fourth Amendment, as adopted, is both brief and ambiguous; it gives no definition and little context to "unreasonable" and does not set forth detailed information regarding the requisite preconditions for the proper issuance of a warrant. *Id*.

Further, it is beyond dispute that the Fourth Amendment, by virtue of the Fourteenth Amendment, prohibits unreasonable searches and seizures by state officers as well as federal officers. Mapp v. Ohio, 367 U.S. 643, 646–48 (1961) (holding that the due process clause of the Fourteenth Amendment extended to the States the Fourth Amendment right against unreasonable searches and seizures, and also extended, inasmuch as necessary to ensure such rights, the exclusionary rule); *see also Elkins*, 364 U.S. at 215 (recounting the history of distinguishing between state and federal actors and discussing the ridiculous outcome that such an analysis creates). According to the Court, no distinction can logically be drawn between evidence obtained in violation of the Fourth Amendment and that obtained in violation of the Fourteenth. *Id*. Moreover, to the victim it matters not whether his constitutional right has been invaded by a federal agent or by a state officer, for "[i]t would be a curiously ambivalent rule that would require the courts of the United States to differentiate between unconstitutionally seized evidence upon so arbitrary a basis. Such a distinction indeed would appear to reflect an indefensibly selective evaluation of the provisions of the Constitution." *Id.*

[23] JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 19 (1966). Our forefathers were less concerned about warrantless searches and more concerned about the issuance of overreaching and overbroad warrants. *Id*. The Court has noted that it is perhaps too much to say that Colonial-Americans "feared the warrant more than the search, but it is plain enough that the warrant was the prime object of their concern. Far from looking at the warrant as a protection against unreasonable searches, they saw it as an authority for unreasonable and oppressive searches." TELFORD TAYLOR, TWO STUDIES IN

stake are necessarily substantial.[24] Thus, the Supreme Court has adamantly reaffirmed that, unless justified by an exception to the warrant requirement, warrantless searches are per se unreasonable.[25]

CONSTITUTIONAL INTERPRETATION 41 (1969). This Colonial struggle includes within its ambit the controversy in England over the issuance of general warrants to aid enforcement of the seditious libel laws and writs of assistance. *See* Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("An important forerunner of the first [ten] Amendments to the United States Constitution, the Virginia Bill of Rights, specifically opposed 'general warrants . . . .' The general warrant was a recurring point of contention in the Colonies immediately preceding the Revolution."); United States v. Chadwick, 433 U.S. 1, 7–8 (1977) ("[T]he Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance . . . [that] granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods."). The Framers' experience and familiarity with the abuses that accompanied the issuance of such general warrants provided the principal stimulus for the restraints on arbitrary governmental intrusions embodied in the Fourth Amendment. *Id.*; *see also* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 40–42 (2008) (providing a detailed account of precisely why American colonists so detested the general warrants of English rule and suggesting that the Fourth Amendment was drafted almost entirely to prevent its reoccurrence is the newly formed United States). Clancy also contends that the warrant was the "initial and primary object" of the Fourth Amendment. *Id.* at 40 n.98. *See generally* TAYLOR, *supra*, at 43 (noting that the history and drafting process of the Fourth Amendment strongly suggest that the warrant was the preeminent object of the amendment).

[24] *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 314–15 (1972) (specially noting the importance of the government and that of the individual). The Court noted that because the Fourth Amendment is not absolute in its terms, it requires a court to examine and balance the basic values at stake in each case—the government's duty to protect domestic security, and the potential danger posed by unreasonable surveillance into individual privacy and free expression. *Id.*

[25] Katz v. United States, 389 U.S. 347, 357 (1967). In *Katz*, the Court noted that it is a well-established doctrine that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Id.* (footnote omitted). The Court has been sure to reaffirm this basic principle whenever the occasion arises. *See* Warden Maryland Penitentiary v. Hayden, 387 U.S. 294, 298–300 (1967) (reiterating that absent exigent circumstances searches without a warrant are unreasonable per se); Cooper v. California, 386 U.S. 58, 59–62 (1967) (same); Stoner v. California, 376 U.S. 483, 486–87 (1964) (same); Chapman v. United States, 365 U.S. 610, 613–15 (1961) (same); Rios v. United States, 364 U.S. 253, 261 (1960) (same); Jones v. United States, 357 U.S. 493, 497–99 (1958) (same); Brinegar v. United States, 338 U.S. 160, 174–77 (1949) (same); McDonald v. United States, 335 U.S. 451, 454–56 (1948) (same); Carroll v. United States, 267 U.S. 132, 153, 156 (1925) (same). Many exceptions to the warrant requirement have developed over the years, but have been, in theory, narrowly tailored and jealously drawn. *See generally* Theodore P. Metzler et al., *Thirtieth Annual Review of Criminal Procedure: Warrantless Searches and Seizures*, 89 GEO. L.J. 1084 (2001) (providing a detailed compilation and analysis of warrantless search and seizure jurisprudence). These exceptions include, but are not limited to

> investigatory detentions, warrantless arrests, searches incident to a valid arrest, seizure of items in plain view, exigent circumstances, consent searches, vehicle searches, container searches, inventory searches, border searches, searches at sea, administrative searches, and

Further, the Court has stressed that all searches should proceed only after issuance of a warrant by a neutral and detached magistrate.[26] To be sure, the Fourth Amendment has two separate and interrelated clauses that coexist to protect citizens from unwarranted governmental intrusion: the "Reasonableness Clause" and the "Warrant Clause."[27] The Court has been careful to note that although the Fourth Amendment speaks broadly of unreasonable searches and seizures, the definition of "reasonableness" turns, at least in part, on the more specific commands of the Warrant Clause.[28]

> searches in which the special needs of law enforcement make the probable cause and warrant requirements impracticable.

Id. at 1084. Other more circumscribed exceptions include warrants to search "pervasively regulated business[es]." United States v. Biswell, 406 U.S. 311, 316 (1972). This also includes warrants to search closely regulated industries "long subject to close supervision and inspection." Colonnade Catering Corp. v. United States, 397 U.S. 72, 77 (1970). One lower court has actually created an explicit list of exceptions to the warrant requirement. *See* State v. Lara, 797 P.2d 296, 303 (N.M. Ct. App. 1990) (noting that warrantless searches are permissible only if they fall within one of the following narrowly drawn exceptions to the warrant requirements: "(1) plain view; (2) probable cause [accompanied by] exigent circumstances; (3) search incident to lawful arrest; (4) consent; (5) hot pursuit; and (6) inventory searches" (citing State v. Ruffino, 612 P.2d 1311 (1980))).

[26] Johnson v. United States, 333 U.S. 10, 13–14 (1948). The Fourth Amendment's protection consists in requiring that inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. *Id*.; *see also* Steagald v. United States, 451 U.S. 204, 212 (1981) (explaining that warrants are necessary because law enforcement "may lack sufficient objectivity to weigh correctly the strength of the evidence supporting the contemplated action"). For instance, in *Coolidge*, the defendant was charged with murder and the chief investigator (and eventual prosecuting attorney), acting in his capacity as justice of the peace, issued a search warrant for defendant's automobile. Coolidge v. New Hampshire, 403 U.S. 443, 449 (1971). The Court found that the seizure and search of the automobile could not constitutionally rest upon the warrant issued by the state official who was not the "neutral and detached magistrate" required by the Constitution because the individual who issued the warrant was also the individual pursuing the case; therefore, the chief investigator/prosecuting attorney lacked the "neutral and detached" quality that is required by the Fourth Amendment. *Id*. (quoting Jackson v. United States, 333 U.S. 10, 13–14 (1948)).

[27] *See* Michigan v. Clifford, 464 U.S. 287, 302 (1984) (Stevens, J., concurring) (referring to the text of the two clauses of the Fourth Amendment); *see also* Kelly A. Borchers, Note, *Mission Impossible: Applying Arcane Fourth Amendment Precedent to Advanced Cellular Phones*, 40 VAL. U. L. REV. 223, 230–31 (2005) (detailing the two clauses of the Fourth Amendment and discussing the interplay between their distinct mandates and implications).

[28] *Keith*, 407 U.S. at 314–15. This includes the fact that a warrant must be reasonable at the time it is issued. *Id*. In *Chimel v. California*, the Court considered the Government's contention that the search be judged on a general "reasonableness" standard without reference to the warrant clause of the Fourth Amendment. 395 U.S. 752, 764–65 (1969). The Court concluded that such an argument was "founded on little more than a subjective view regarding the acceptability of certain sorts of police conduct, and not on considerations relevant to Fourth Amendment interests." *Id*. The Court was deeply concerned that

The initial clause of the Fourth Amendment is known as the "Reasonableness Clause" and has been understood to state a comprehensive principle—the government shall not violate the "right to be secure" by conducting "unreasonable" searches and seizures.[29] This portion of the Amendment explains who and what the Fourth Amendment envelopes (i.e., protection of "the people" and their "persons, houses, papers, and effects").[30] The latter portion of the Amendment is known as the "Warrant Clause" because it relates specifically to warrants and explains what a court requires before it issues a warrant.[31]

1. The Warrant Requirement

The warrant requirement of the Fourth Amendment contains two separate and independent standards: (1) there must be probable cause for the warrant to be issued, and (2) the warrant must particularly

---

"[u]nder such an unconfined analysis, Fourth Amendment protection in this area would approach the evaporation point." *Id*. at 765. The Court has also noted that the warrant requirement is far from superfluous language and has reiterated its value as a part of our constitutional law for decades. *Keith*, 407 U.S. at 315–16; *Coolidge*, 403 U.S. at 481. It has emphatically noted that the warrant requirement is not a mere "inconvenience to be somehow 'weighed' against the claims of police efficiency." *Keith*, 407 U.S. at 315 (quoting *Coolidge*, 403 U.S. at 481). "It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' . . . of law enforcement." *Id*. at 315–16 (quoting *Coolidge*, 403 U.S. at 481).

[29] Davies, *supra* note 21, at 557, 574. Numerous commentaries discuss the fundamental meanings of the Fourth Amendment clauses, the interplay between them, and the inherent difficulties that arise when attempting to reconcile them. *Id*. For a more in-depth discussion, see 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 5–7 (3d ed. 1996) [hereinafter LAFAVE, TREATISE ON THE FOURTH AMENDMENT] (discussing the interaction between these two Fourth Amendment clauses).

[30] U.S. CONST. amend. IV; JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE § 6.01 (3d ed. 2002).

[31] *See* Borchers, *supra* note 27 (providing analysis as to how the Warrant and Reasonableness Clauses relate to one another). The Warrant Clause requires that warrants should only be issued upon "probable cause, supported by Oath or affirmation" and that the warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV; *see also* New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) (quoting Almeida-Sanchez v. United States, 413 U.S. 266, 277 (1973)) (finding that although in certain limited circumstances a warrant is not required, "[t]he fundamental command of the Fourth Amendment is that searches and seizures be reasonable, and . . . the requirement of a warrant bear[s] on the reasonableness of a search"); Berger v. New York, 388 U.S. 41, 86 (1967) (holding that searches and seizures are presumptively unconstitutional unless conducted pursuant to a valid warrant). In *Steele v. United States*, the Court held that a warrant should describe the places to be searched and objects to be seized with sufficient particularity so as to leave nothing to the discretion of the officer executing the warrant. 267 U.S. 498, 503 (1925).

describe who or what is to be seized.[32] Initially, probable cause is an objective concept that attempts to circumscribe the power of the government in obtaining warrants by requiring, at minimum, a loose nexus between the alleged criminal activity, the items to be seized, and the place to be searched.[33] The second requirement—the particularity requirement—provides that the warrant describe the places to be searched and objects to be seized with sufficient particularity so that officers may "with reasonable effort ascertain and identify the place [or object] intended."[34] The degree of specificity required will vary with the specific facts of the case; nonetheless, the Supreme Court resolutely

---

[32] *Steele*, 267 U.S. at 503; *see also infra* Part II.A.2 (providing an in-depth discussion of the particularity requirement).

[33] *See generally Steele*, 267 U.S. at 499–502 (recounting painstakingly the process by which an official obtains a warrant for probable cause). Probable cause is viewed as a static concept due to its objective nature. Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 954–56 (2003). Thus, no amount of subjective belief on behalf of law enforcement is sufficient to meet the standards of probable cause; there must exist "objective probable cause." DRESSLER, *supra* note 30, § 9.02; *see also* Whren v. United States, 517 U.S. 806, 813 (1996) (holding that a law enforcement official's motives are not a factor when determining probable cause but are a factor when determining the reasonableness of a search, the extent of a search, or the manner in which a search was conducted). For the purposes of this Note, it is assumed that the probable cause requirement has been met. Probable cause is considerably less of an issue in the context of Fourth Amendment cases involving the search and seizure of computer or digital evidence.

[34] *Steele*, 267 U.S. at 503; *see also, e.g.*, United States v. Rogers, 150 F.3d 851, 855 (8th Cir. 1998) (finding warrant sufficiently particular even though it contained directions that omitted the final turn because the surrounding property did not fit description of house in warrant); United States v. Butler, 71 F.3d 243, 249 (7th Cir. 1995) (finding warrant sufficiently particular although the first floor was not listed because affidavit supported conclusion that all three floors were under control of the target of the warrant); United States v. Gilliam, 975 F.2d 1050, 1055 (4th Cir. 1992) (finding warrant sufficiently particular although it contained an erroneous description of one of the farm's boundaries because the warrant contained information that targeted the only farm in the vicinity and was thus sufficiently particular to avoid the risk of searching the wrong property); United States v. Dancy, 947 F.2d 1232, 1234 (5th Cir. 1991) (finding warrant sufficiently particular where it merely contained the correct street address). *But see, e.g.*, Bartholomew v. Pennsylvania, 221 F.3d 425, 426 (3d Cir. 2000) (finding warrant insufficiently particular where it did not state items to be seized because attached exhibit listing items was sealed); United States v. Shamaeizadeh, 80 F.3d 1131, 1137 (6th Cir. 1996) (finding warrant insufficiently particular because officers had actual notice that the house was divided into two apartments prior to conducting search, yet failed to list the basement apartment); United States v. Dahlman, 13 F.3d 1391, 1395–96 (10th Cir. 1993) (finding warrant insufficiently particular because location was identified by only two lot numbers within subdivision and without reference to structures on property); United States v. Ellis, 971 F.2d 701, 703–04 (11th Cir. 1992) (finding warrant insufficiently particular because it lacked a physical description of the premises, merely identifying it as the "third mobile home on the north side"); United States v. Nafzger, 965 F.2d 213, 215–16 (7th Cir. 1992) (per curiam) (finding warrant insufficiently particular because it identified locus of the search for a truck as "Western District of Wisconsin").

advocates that officers must procure a warrant before conducting a search or seizure.[35]

2. The Particularity Requirement

The particularity requirement of the Fourth Amendment serves two major functions: (1) it informs the officers of what they are allowed to lawfully search and seize, and (2) it notifies the person who is being searched or seized of what the officers are lawfully allowed to take.[36] The particularity requirement is especially important in the context of digital evidence because it demarcates the boundaries of a given search.[37]

---

[35] *See* Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) (noting that the necessity of drawing Fourth Amendment exceptions as narrowly as possible "may appear unrealistic or 'extravagant' to some. But the values were those of the authors of our fundamental constitutional concepts," and that "[i]n times not altogether unlike our own [our forefathers] won . . . a right of personal security against arbitrary [invasions] by official power"); Katz v. United States, 389 U.S. 347, 357 (1967) (emphasizing that the most basic constitutional norm in this area is "that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment" and that such exceptions are jealously and carefully drawn); Gouled v. United States, 255 U.S. 298, 303–04 (1921) ("It would not be possible to add to the emphasis with which the framers of our Constitution and this court have declared the importance . . . of the due observance of the rights guaranteed under the Constitution by [the Fourth Amendment]." (citations omitted)).

[36] United States v. Chadwick, 433 U.S. 1, 9 (1977) (holding that particular warrants ensure that the target of the search or seizure is aware of what police may search, their reasons for doing so, and the appropriate limits to the search); Hon. Robert H. Bohn, Jr. & Lynn S. Muster, *The Dawn of the Computer Age: How the Fourth Amendment Applies to Warrant Searches and Seizures of Electronically Stored Information*, 8 SUFFOLK J. TRIAL & APP. ADVOC. 63, 65 (2003). A particular warrant also informs the individual subject to the search or seizure "of the lawful authority of the executing officer, his need to search, and the limits of his power to search." Groh v. Ramirez, 540 U.S. 551, 561 (2004) (citing *Chadwick*, 433 U.S. at 9). This also acts as a check on the administrative arm of the government. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

[37] United States v. Young, 745 F.2d 733, 759 (2d Cir. 1984). A warrant is sufficiently particular if it "enable[s] the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." United States v. George, 975 F.2d 72, 75 (2d Cir. 1992).

> Courts tend to tolerate a greater degree of ambiguity where law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.

United States v. Buck, 813 F.2d 588, 590 (2d Cir. 1987) (quoting *Young*, 745 F.2d at 759); *see also* United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the

The Supreme Court has explicitly recognized that the interests served by the requirement suggest that it should be somewhat flexible and malleable, requiring reasonable specificity.[38] In *Katz v. United States*, the Court determined that no discretion should be left to the executing officers; thus, even if officers act with restraint, the warrant may be found unconstitutional because the restraint is to be imposed by a neutral and detached magistrate rather than law enforcement officials.[39]

---

items subject to seizure is not possible."). However, "[a] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *George*, 975 F.2d at 76.

[38] Marron v. United States, 275 U.S. 192 (1927); Hon. Bohn, Jr. & Muster, *supra* note 36, at 65 (2003); *see also Steele*, 267 U.S. at 503 (stating that the place to be searched must be described to such an extent that an officer can identify it by using only reasonable effort). Thus it is sufficiently particular to simply state the street address of a house that is to be searched, but more may be required if the location is a multi-unit complex. *See Garrison*, 480 U.S. at 80–81 (finding that where a search warrant specified the location of the search as "the premises known as 2036 Park Avenue third floor apartment" and two apartments actually existed at such address, the search warrant was not held invalid because officers "reasonably concluded that there was only one apartment on the third floor" based on objective facts). The Supreme Court has found that the interests served by the particularity requirement of the Fourth Amendment are "to prevent general searches, to prevent the seizure of one thing under a warrant describing another, and to prevent warrants from being issued on vague or dubious information." *Groh*, 540 U.S. at 560; *see also Coolidge*, 403 U.S. at 467 (noting that the particularity requirement protects against "general, exploratory rummaging in a person's belongings"). Generally, warrants are found to be *insufficiently* particular where "[n]othing on the face of the warrant tells the searching officers for what crime the search is being undertaken." *George*, 975 F.2d at 76; *see also* United States v. Bianco, 998 F.2d 1112, 1116 (2d Cir. 1993) (finding warrant lacked particularity where it did not describe "the possible crimes involved"); United States v. Hickey, 16 F. Supp. 2d 223, 240 (E.D.N.Y. 1998) (invalidating several warrants on particularity grounds where "none identified the nature of the suspected wrongdoing triggering the searches"); Roberts v. United States, 656 F. Supp. 929, 935 (S.D.N.Y. 1987) (finding warrant insufficiently particular where, among other omissions, the warrant contained "no restriction to any specific wrongful transaction to which the documents were related"), *rev'd on other grounds*, 852 F.2d 671 (2d Cir. 1988).

[39] *See Katz*, 389 U.S. at 356 (holding that antecedent judicial authorization, not given in the instant case, was a constitutional precondition of the kind of electronic surveillance involved). The Court in *Katz* took the opportunity again to stress that "[s]earches conducted without warrants have been held unlawful 'notwithstanding facts unquestionably showing probable cause,'" that the "Constitution requires . . . [']the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police,'" that "'[o]ver and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment." *Id*. at 357 (fourth alteration in original) (citations omitted). *See Groh*, 540 U.S. at 560 (noting that the Warrant Clause's main protection is that it has "interposed a magistrate between the citizen and the police. . . . so that an objective mind might weigh the need to invade [the searchee's] privacy in order to enforce the law" (quoting McDonald v. United States, 335 U.S. 451, 455 (1998))); *see also*

As well as struggling to find the right scope of particularity within the Fourth Amendment, courts have also struggled with the exact meaning of the terms "search" and "seizure" within the purview of Fourth Amendment jurisprudence.[40]

3. What Constitutes a "Seizure"?

The Court has defined a seizure as a "meaningful interference with an individual's possessory interests" in property.[41] Thus, a seizure occurs when an officer removes or destroys property or when she secures the premises where property is located, because these actions meaningfully interfere with an individual's property rights.[42] Likewise,

---

Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997) (noting that a warrant may be valid if it describes the items to be seized in broad or generic terms and "when the description is as specific as the circumstances and the nature of the activity under investigation permit" (quoting United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988))); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment . . . .").

40 Darla W. Jackson, *Protection of Privacy in the Search and Seizure of E-Mail: Is the United States Doomed to an Orwellian Future?*, 17 TEMP. ENVTL. L. & TECH. J. 97, 100, 102 (1999); *see also* Minnesota v. Carter, 525 U.S. 83, 98 (1998) (Scalia, J., concurring) (noting that the meaning of the terms is "not remotely contained in the Constitution"); *infra* Part II.A.3 (discussing the precise meaning of the terms "search" and "seizure" within the context of the Fourth Amendment).

41 Maryland v. Macon, 472 U.S. 463, 469 (1985) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)); *see also* United States v. Place, 462 U.S. 696, 708–09 (1983) (finding that the term "seizure" signifies a meaningful interference with possessory interests or property rights); Texas v. Brown, 460 U.S. 730 (1983) (Stevens, J., concurring) (same); *Chadwick*, 433 U.S. at 13–14, 14 n.8 (same); Hale v. Henkel, 201 U.S. 43, 76 (1906) (same). Although the concept of a "seizure" of property is actually discussed fairly infrequently by the Court, its definition flows from "[the Court's] oft-repeated definition of the 'seizure' of a person within the meaning of the Fourth Amendment." *Jacobsen*, 466 U.S. at 113 n.5. That is the "meaningful interference, however brief, with an individual's freedom of movement." *Id.*; *see also* Michigan v. Summers, 452 U.S. 692, 696 (1981) (finding that a seizure implicates a meaningful interference with possessory or property interests); Reid v. Georgia, 448 U.S. 438, 440 (1980) (per curiam) (same); United States v. Mendenhall, 446 U.S. 544, 551–54 (1980) (Stewart, J.) (same); Brown v. Texas, 443 U.S. 47, 50 (1979) (same); United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975) (same); Cupp v. Murphy, 412 U.S. 291, 294–95 (1973) (same); Davis v. Mississippi, 394 U.S. 721, 726–27 (1969) (same); Terry v. Ohio, 392 U.S. 1, 16, 19 n.16 (1968) (same).

42 *See, e.g.*, Soldal v. Cook County, 506 U.S. 56, 60 (1992) (holding that, where a landlord chose to forcibly evict a tenant two weeks prior to the scheduled eviction hearing by removing and selling the tenants' trailer, the seizure of the trailer implicated the tenant's privacy and liberty interests that were protected under the Fourth Amendment because the eviction involved sufficient state action); *Jacobsen*, 466 U.S. at 120–21 (holding that a seizure resulted where federal agents exhibited dominion over a white powdery substance found in the innermost of a series of four plastic bags that had also been concealed in a tube inside

due to a similar lack of interference, a seizure does not occur when an officer merely picks up and immediately sets down an object.[43]

In *United States v. Jacobsen*, for instance, Federal Express employees, while inspecting a package that was damaged and torn by a forklift, encountered tubes containing plastic bags with white powder; they promptly returned the contents of the tube and notified the Drug Enforcement Administration.[44] Upon arrival, a federal agent noticed the box, now re-wrapped, on the table with a hole; he removed the plastic bags from within and conducted a field test on the substance.[45] The Court held that the officer's "assertion of dominion and control over the package and its contents" qualified as a "seizure" for Fourth Amendment purposes.[46] Conversely, in *Arizona v. Hicks*, where the investigating officers moved stereo equipment to view the serial number underneath, the Court held that no seizure occurred because the slight movement did not meaningfully affect the individual's possessory interests.[47] Thus, the Supreme Court has devised a logical and workable

---

of a damaged package, but nonetheless allowing the warrantless seizure because it was not unreasonable); *Place*, 462 U.S. at 707–09 (holding that officials' conduct constituted a "seizure" of traveler's luggage when, following his refusal to consent to a search, a government agent told the traveler that he was going to take the luggage to a federal judge to procure a search warrant); *Terry*, 392 U.S. at 19 (holding that officer "seized" defendant and subjected him to a "search" when he took hold of him and patted down the outer surface of his clothing); Pepper v. Village of Oak Park, 430 F.3d 805, 809 (7th Cir. 2005) (holding that the permanent taking of owner's television set and substantial damage to her couch amounted to "seizure" under Fourth Amendment).

43 *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 328 (1987) (holding that where an officer was in a home pursuant to exigent circumstances—a bullet had been fired into it from the apartment below—and the officer moved some components of stereo equipment in order to read and record their serial numbers, a search but not a seizure had occurred for purposes of the Fourth Amendment).

44 466 U.S. at 111.

45 *Id.* at 111–12.

46 *Id.* at 120. Likewise, and for the first time, the Supreme Court unanimously held that during a traffic stop, a car and all of its occupants—not just the driver—are "seized" for purposes of the Fourth Amendment. Brendlin v. California, 551 U.S. 249, 263 (2007). Thus, the concept of a "meaningful interference" applies to both meaningful interference of property rights and the meaningful interference of the individual to move freely. *See id.* at 254 (noting that "[a] person is seized by the police and thus entitled to challenge the government's action under the Fourth Amendment when the officer, ' 'by means of physical force or show of authority,' ' terminates or restrains his freedom of movement" (citing Florida v. Bostick, 501 U.S. 429, 434 (1991))).

47 480 U.S. at 324. The Court did, however, hold that the action taken by the officers was a "search" within the Fourth Amendment because such actions exposed to view previously concealed portions of the apartment and its contents, and produced a new invasion of privacy that was unjustified by the exigent circumstance validating the initial entry. *Id.* at 325.

definition of what constitutes a seizure for purposes of the Fourth Amendment.[48]

B. Exceptions to the Warrant Requirement: The Plain View Exception

Although the text of the Fourth Amendment prohibits unreasonable searches and seizures, it does not expressly require the government to obtain a warrant in order to conduct a search or seizure; nevertheless, the Court has held that warrantless searches and seizures are per se unreasonable unless justified by an exception.[49] The rigidity with which the bounds of such exceptions should be drawn is debatable; however, it remains true that warrants are highly preferred.[50] Nevertheless, over the

---

[48] *See supra* notes 41–47 and accompanying text (discussing the concept of "seizure" as a meaningful interference with the possessory interest of the individual or a meaningful interference of the individual's freedom of movement).

[49] Katz v. United States, 389 U.S. 347, 357 (1967); *see also* DRESSLER, *supra* note 30, §§ 12–17 (providing a detailed and in-depth analysis of the jurisprudence surrounding the major exceptions to the warrant requirement of the Fourth Amendment).

[50] *See Katz*, 389 U.S. at 357 (holding that even when justified by probable cause, warrantless searches are unreasonable per se "subject only to a few specifically established and well-delineated exceptions"). The axiom that warrantless searches are per se unreasonable absent exigent circumstances is oft-repeated in Fourth Amendment cases and is truly a cornerstone of Fourth Amendment jurisprudence. *See* Arizona v. Gant, 129 S. Ct. 1710, 1716 (2009) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (quoting *Katz*, 389 U.S. at 357)); Pearson v. Callahan, 129 S. Ct. 808, 810 (2009) ("[U]nder this Court's clearly established precedents, warrantless entries into a home are *per se* unreasonable [absent] exigent circumstances."); Georgia v. Randolph, 547 U.S. 103, 109 (2006) ("To the Fourth Amendment rule ordinarily prohibiting the warrantless entry of a person's house as unreasonable *per se*, one 'jealously and carefully drawn' exception . . . [is] voluntary consent . . . ." (citations omitted) (quoting Jones v. United States, 357 U.S. 493, 499 (1958))); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) ("[A] search conducted without a warrant issued upon probable cause is '*per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions.'" (omission in original) (quoting *Katz*, 389 U.S. at 357)); Chambers v. Maroney, 399 U.S. 42, 51 (1970) ("[The Court requires] the judgment of a magistrate on the probable-cause issue and the issuance of a warrant before a search is made. Only in exigent circumstances will the judgment of the police as to probable cause serve as a sufficient authorization for a search."); United States v. Jeffers, 342 U.S. 48, 51 (1951) (stating that "[o]nly where incident to a valid arrest, or in 'exceptional circumstances,' may an exemption lie" from judicial processes required by Fourth Amendment (citations omitted)); Agnello v. United States, 269 U.S. 20, 33 (1925) ("Belief, however well founded, that an article sought is concealed in a dwelling house, furnishes no justification for a search of that place without a warrant."). In order to avoid having to address the issue, some courts interpret even arguably narrow warrant language into broader discretionary language in the context of computer searches and seizures. *See* United States v. Gleich, 293 F. Supp. 2d 1082, 1089 (D.N.D. 2003) (holding that a search of three computers did not exceed the scope of a warrant because the warrant authorized a search and seizure of items that could contain "photographs, pictures, visual

years the Court has developed many exceptions to the warrant requirement.[51] One exception that is frequently used and has become considerably recognized is a law enforcement official's ability to seize an object of apparently incriminating nature without a warrant so long as it is in "plain view" and the official is lawfully present.[52] Like "seizure," "plain view" is a term of art that has substantial development within Fourth Amendment jurisprudence.[53]

An object that is in "plain view" of a law enforcement official may be seized without a warrant if (1) the official views the object from a lawful

---

representations, or videos in any form that include sexual conduct by a minor, as defined by [state statute]"); United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986) (holding narcotics agents did not exceed the scope of the warrant in seizing computer disks not described in the warrant because "in the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take" (quoting United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986))); People v. Gall, 30 P.3d 145, 153–54 (Colo. 2001) (holding that laptop computers are "reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material'" and therefore fell within the scope of a warrant that authorized the search of written or printed material).

[51] *See* ROBERT M. BLOOM & MARK S. BRODIN, CONSTITUTIONAL CRIMINAL PROCEDURE § 6 (1992) (providing a comprehensive list—to the extent any list can be comprehensive in this area—and analyzing the relevant case law pertaining to the many exceptions to the warrant requirement of the Fourth Amendment).

[52] *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (enunciating, for the first time, the Court's interpretation of the plain view doctrine). The common thread among "plain view" cases is that the official in question had a previous justification for an intrusion or invasion and in the course of such he inadvertently came across a piece of incriminating evidence. *See id.* at 466. According to *Coolidge*, the plain view doctrine supplements the prior justification—whatever the reason—and allow for the seizure. *Id.* The Court cautioned that the "original justification is legitimate only where it is immediately apparent to the police that they have evidence before them," and that the "'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." *Id.*

[53] *See id.* at 464–66 (carving out the intricacies of the plain view doctrine after discussing the similarities amongst lower court decisions and outlining the "circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal."). The *Coolidge* plurality opinion, which brought the inception of the plain view doctrine and is among the most cited cases in plain view jurisprudence, noted that under certain circumstances the police may lawfully seize evidence in plain view without a warrant, but that it is important to remember that "in the vast majority of cases, *any* evidence seized by the police will be in plain view, at least at the moment of seizure," and that the most difficult aspect of the doctrine "has been to identify the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal." *Id.* at 465. The Court further recognized that the particularity clause and the notion that no amount of probable cause can justify a warrantless search or seizure absent exigent circumstances prohibits use of the plain view doctrine on items for which officers have probable cause from the outset. *Id.* at 464–65. Consequently, the inadvertency requirement, to Justice Stewart, is merely a shorthand reference to existing Fourth Amendment jurisprudence. *See id.*

vantage point; (2) the official has a right of physical access to it; and (3) it is immediately apparent that the object is unlawful by its character or nature.[54] Importantly, the doctrine does not serve as an exception to

[54] *Id.* at 466. Originally, the plain view exception contained the additional requirement that the officer also come across the evidence "inadvertently." *Id.* at 466–67. The Court later trimmed this requirement from its plain view analysis. *See* Horton v. California, 496 U.S. 128, 137–38 (1990) (concluding that the inadvertence requirement of the plain view doctrine should no longer be analyzed as part of the application because it would be surplusage). According to the *Coolidge* plurality opinion, the plain view doctrine is most generally applicable when "the police have a warrant to search a given area for specified objects, and in the course of the search [inadvertently] come across some other article of incriminating character." *Coolidge*, 403 U.S. at 465; *see also Horton*, 496 U.S. at 137 (noting that "[the officer] must also have a lawful right of access to the object itself" in order to seize evidence pursuant to the plain view exception); Washington v. Chrisman, 455 U.S. 1, 5–6 (1982) (noting that "[t]he 'plain view' exception . . . permits a law enforcement officer to seize what clearly is incriminating evidence or contraband when it is discovered in a place where the officer has a right to be" (citing *Coolidge*, 403 U.S. 443)). Interestingly, prior to *Horton*, each and every circuit court had issued a decision that cited the inadvertent requirement favorably. *E.g.*, United States v. Caggiano, 899 F.2d 99, 103 (1st Cir. 1990); United States v. Poulos, 895 F.2d 1113, 1121 (6th Cir. 1990); United States v. Barrios-Moriera, 872 F.2d 12, 16 (2d Cir. 1989); Crowder v. Sinyard, 884 F.2d 804, 826 n.30 (5th Cir. 1989); United States v. Holzman, 871 F.2d 1496, 1512 (9th Cir. 1989); United States v. Peterson, 867 F.2d 1110, 1113 (8th Cir. 1989); United States v. Meyer, 827 F.2d 943, 945 (3d Cir. 1987); Wolfenbarger v. Williams, 826 F.2d 930, 935 (10th Cir. 1987); Tarantino v. Baker, 825 F.2d 772, 777 n.3 (4th Cir. 1987); United States v. Perry, 815 F.2d 1100, 1105 (7th Cir. 1987); United States v. Bent-Santana, 774 F.2d 1545, 1551 (11th Cir. 1985); *In re* Search Warrant for Premises at 2125 S. Street, Northwest, Washington, D.C., 667 F.2d 117, 145 (D.C. Cir. 1981). Further, forty six of the fifty states had adopted the inadvertent discovery requirement as a part of Fourth Amendment plain view analysis. *See Horton*, 496 U.S. at 145 n.2 (Brennan, J. & Marshall, J., dissenting) (collecting cases) ("Only three States—California, Idaho, and Utah—have rejected the inadvertent discovery requirement."). It is also interesting to note that California and Idaho are located within the Ninth Circuit, and Utah is within the Tenth Circuit—both having since adopted a view very similar to the inadvertent discovery requirement when the doctrine is applied to computer searches and seizures. *See Comprehensive Drug Testing III*, 579 F.3d 989, 995 (9th Cir. 2009) (en banc) (holding that the government should completely forswear use of the plain view doctrine or any similar doctrine in the context of computer-based evidence cases), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc); United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (implementing a "special approach" that inquires as to the subjective intent of the officer at the time of the plain view sighting). Moreover, even the courts that have not adopted the inadvertent discovery requirement have concluded that the government may not engage in pretextual searches—a concept intimately related to inadvertent discovery. *See* State v. Bussard, 760 P.2d 1197, 1204 n.2 (Idaho Ct. App. 1988) (holding that an officer who enters area pursuant to a warrant to search for evidence of one crime when he is really interested only in seizing evidence relating to another crime for which he does not have a warrant, has engaged in a "pretextual" search and the fruits of that search should be suppressed); State v. Kelly, 718 P.2d 385, 389 n.1 (Utah 1986) (holding the same).

Fourth Amendment searches but rather serves to justify seizures of incriminating evidence that is in plain view.[55]

The initial requirement for the seizure of evidence in plain view is that the officer must be lawfully present when she views the evidence.[56] Most evidence seized pursuant to the plain view doctrine is seized either (1) during the execution of a valid search warrant, or (2) during a search justified by an exception to the warrant requirement.[57] The second requirement under plain view analysis requires that the official have a lawful right of access to the object.[58] The third and final requirement is

---

[55] *Coolidge*, 403 U.S. at 466 (noting that "[t]he doctrine serves to supplement the prior justification . . . and permits the warrantless seizure"). The Court was careful to note, however, that the extension of the prior justification is legitimate only where it is immediately apparent to the police that they have evidence before them. *Id*. The plain view doctrine, according to the Court, cannot be used "to extend a general exploratory search from one object to another until something incriminating at last emerges." *Id*.

[56] *Horton*, 496 U.S. at 136.

[57] *Id*. at 135. Suppose, for instance, that police obtain a valid warrant to search defendant's home based on probable cause that she was involved in a homicide, and therein they find marijuana strewn across the coffee table. The plain view doctrine would allow the seizure of the marijuana—although a strict reading of the Fourth Amendment would not allow it—because the amendment recognizes that the delay, inconvenience, and risk of destruction of evidence require the procurement of a warrant. *See* BLOOM & BRODIN, *supra* note 51, § 6.8 (1992) (providing essentially the same hypothetical example). The officer is allowed to seize the contraband without obtaining a warrant because, among other things, she was lawfully present pursuant to a valid search warrant, which satisfies the first prong of the plain view inquiry. *See id*. Suppose instead that the police did not have a valid warrant to search the home, but the defendant consented to their entry and they subsequently found the drugs. The police could likewise seize the evidence because they were lawfully present pursuant to a well recognized exception to the warrant requirement—consent. *See id.* Suppose now, however, that the searching officers do not enter the house pursuant to a valid warrant or exception to the warrant requirement, but are merely conducting their routine foot patrol of the neighborhood when they observe the marijuana lying on the coffee table through an open window. The officers would not be able to enter the home and seize the contraband absent a warrant because the plain view requirement will only authorize the seizure *after* the officers have lawfully entered the premises. *See id*. The plain view doctrine *will not* provide the justification for the initial entry upon the premises. *Id.*

[58] BLOOM & BRODIN, *supra* note 51, § 6.8. Bloom and Brodin also state that this requirement mandates that the object be "observed while the officer is confining her activities to the permissible scope of [the initial] intrusion." *Id.*; *see also Coolidge*, 403 U.S. at 468 (noting that even where the evidence is in plain view, the "Court has repeatedly stated and enforced the basic rule that the police may not enter [private premises] and make a warrantless seizure"). In *Washington v. Chrisman*, a police officer arrested the defendant for possessing alcohol as a minor and asked for his identification. 455 U.S. at 3. The defendant responded that his identification was in his room but that the officer could accompany him while he went to retrieve it. *Id*. As the defendant entered his dorm room to obtain his identification, the officer leaned against the doorjam and waited. *Id*. at 5–7. From the doorway the officer noticed seeds and a pipe lying on the desk inside the room, and from his training was quite sure they were marijuana related. *Id.* The officer seized the evidence

that the criminal nature of the evidence must be "immediately apparent."[59] This third prong plays a vital role in determining whether evidence may be seized pursuant to the plain view exception to the warrant requirement.[60] Although no longer an element of plain view

---

and the defendant appealed alleging that the officer had no right to access the drugs within his room. *Id.* The Court held that the officer had a right to accompany the arrestee to his room closely and keep an eye on him at all times. *Id.* Therefore, the Court reasoned that because the officer was lawfully present at his vantage point (i.e., the doorway) he had a right to seize the evidence. *Id.* at 9. The Court noted that this was "a classic instance of incriminating evidence found in plain view when a police officer, for unrelated but entirely legitimate reasons, obtains lawful access to an individual's area of privacy," and that "[t]he Fourth Amendment does not prohibit seizure of evidence of criminal conduct found in these circumstances." *Id.* The dissent took a different approach, claiming that although the officer had a right to stand in the doorway to keep an eye on the arrestee, he did not have the same right to enter the room *for the purpose of investigating his suspicion about the seeds and pipe*. *Id.* at 10–11 (White, J. dissenting, joined by Brennan & Marshall, JJ.). The Court expressly distinguished the officer's right to be present in the doorway from an officer that might have merely been passing through the hallway while the defendant's door was open stating "[t]he circumstances of this case distinguish it significantly from one in which an officer, who happens to pass by chance an open doorway to a residence, observes what he believes to be contraband inside." *Id.* at 9 n.5; *see also, e.g.*, Payton v. New York, 445 U.S. 573, 585–89 (1980) (holding that the Fourth and Fourteenth Amendments prohibit the police from making a warrantless, nonconsensual entry into a suspect's home to make a routine felony arrest because such an arrest was an invasion of the sanctity of the home, absent exigent circumstances, even when it was accomplished under statutory authority and when probable cause was present); Johnson v. United States, 333 U.S. 10, 14–15 (1948) (holding that where police smelled opium from outside a door, the warrantless arrest and search violated the Fourth Amendment even though officers may have had probable cause to obtain a search warrant because no exigent circumstances existed and the inconvenience and slight delay in preparing papers and presenting the evidence to a magistrate does not justify bypassing the warrant requirement).

[59] Minnesota v. Dickerson, 508 U.S. 366, 375 (1993). In *Dickerson*, the Supreme Court explained that the incriminating nature of an object is immediately apparent if police have probable cause to believe an object in plain view is contraband. *Id*. To illustrate, in *Coolidge*, law enforcement officials seized defendant's car from his driveway because they thought it might implicate him in a crime. 403 U.S. at 446. Upon a microscopic search of the vehicle the police found incriminating evidence, but because the criminal nature of the evidence was not "immediately apparent"—that is, the police had to employ extrinsic means to establish the criminal nature of the evidence—the Court held the seizure to be invalid. *Id*. at 472–74. Likewise, in *Arizona v. Hicks*, the police entered the defendant's apartment pursuant to a valid search warrant and while inside moved a piece of stereo equipment to see the serial number underneath, later confirming via the number that the equipment was stolen. 480 U.S. 321, 327 (1987). The Court found the search was unconstitutional because the serial number was not "immediately apparent" as the equipment had to be moved before it was able to be viewed. *Id*.

[60] *See* David S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 868–70 & n.198 (2005) (discussing the importance of the "immediately apparent" requirement in plain view analysis). However, some courts have been willing to apply the "immediately apparent" requirement in a less than strict manner. *See, e.g.*, United States v. Khabeer, 410 F.3d 477, 482 (8th Cir. 2005) (allowing, under the plain view exception, receipts and identity documents beyond

analysis, the Court once held that the evidence seized pursuant to the plain view doctrine had to be found inadvertently.[61] Regardless, it is important to remember that the plain view exception, by itself, will never justify an entry onto private premises.[62]

1. Digital Evidence Creates Novel Difficulties

Unlike the "papers" and "effects" that the Framers of the Fourth Amendment originally contemplated, computers and other devices that store digital evidence can hold an enormous amount of data.[63] Moreover, people use computers for almost everything imaginable—from storing videos, pictures, and personal records to corresponding with individuals worldwide.[64] Although computer and digital data is in

---

the scope of the warrant in a fraud case); United States v. Calle, No. 98-50377, 1999 WL 313361 (9th Cir. Mar. 22, 1999) (holding travel documents admissible under the plain view exception because the officer read the documents and saw that the dates on them were inconsistent with defendant's prior statements); United States v. Calloway, 116 F.3d 1129, 1133 (6th Cir. 1997) (holding notes, bank receipts, and power of attorney found during search for other types of documents evidencing aircraft piracy admissible under plain view exception).

61 *See Coolidge*, 403 U.S. at 467–471 & n.26 (holding that inadvertent discovery is necessary to plain view analysis because it is the logical manifestation of the Fourth Amendment's explicit constitutional protections: (1) that a magistrate's detached probable cause determination is mandatory, and (2) that searches and seizures deemed necessary are as narrow and limited as possible); *see also supra* notes 52–54 (discussing the initial implementation and subsequent tailoring of the inadvertent discovery requirement). Justice Stewart's opinion deemed that if the Court is going to allow warrantless seizures of evidence in plain view, the inadvertent discovery requirement is a necessary limitation to such an exception. *Coolidge*, 403 U.S. at 468. Justice Stewart concluded that the first limitation on the doctrine is that plain view alone is never enough to justify a seizure because absent exigent circumstances there exists no rational basis for excusing the warrantless seizure; and, second, that the discovery of evidence must be inadvertent because where police know in advance of the evidence and intend to seize it, they should obtain a warrant particularly describing it. *Id.* at 468–69. Thus, the inadvertent discovery requirement, according to Justice Stewart, was the logical manifestation of the warrant requirement and the particularity requirement of the Fourth Amendment. *See id.* at 467–71.

62 *See Coolidge*, 403 U.S. at 469 ("[P]lain view *alone* is never enough to justify the warrantless seizure of evidence. This is simply a corollary of the familiar principle discussed above, that no amount of probable cause can justify a warrantless search or seizure absent 'exigent circumstances.'").

63 *See* United States v. Cioffi, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) ("The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because '[c]omputers . . . often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize.'" (omission in original) (quoting United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 (S.D.N.Y. 2007))).

64 *See Comprehensive Drug Testing III*, 579 F.3d 989, 1005 (9th Cir. 2009) (en banc) ("Electronic storage and transmission of data is no longer a peculiarity or luxury of the very rich; it's a way of life."), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010)

some ways comparable to traditional physical evidence, inherent differences make any straight-forward comparison troubling.[65] The Ninth Circuit in *United States v. Comprehensive Drug Testing*, suggested that the problem is stated quite simply as follows: "There is no way to be sure exactly what an electronic file contains without somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique."[66] Further, relevant electronic files are stored on media along with, at times, millions of other files.[67] By necessity, then, government efforts to locate particular evidence will require examination of many irrelevant files to ensure that the desired data is not overlooked or hidden.[68]

Some courts have likened computers to file cabinets or other closed containers and applied existing Fourth Amendment case law to

---

(en banc); United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006) ("Computers are simultaneously file cabinets . . . and locked desk drawers; they can be repositories of . . . deeply personal information, but also of evidence of crimes. . . . As society grows ever more reliant on computers . . . courts will be called upon to analyze novel legal issues and develop new rules within . . . Fourth Amendment jurisprudence.").

65 *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer."); United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("With their unparalleled ability to store and process information, computers are increasingly relied upon by individuals in their work and personal lives. Computer searches present [similar problems]—the intermingling of relevant and irrelevant material—but to a heightened degree."); *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005) (arguing that new dynamics of computer crime should result in the creation of new doctrines that "impose some new restrictions on police conduct").

66 *Comprehensive Drug Testing III*, 579 F.3d at 1004; *see also Walser*, 275 F.3d at 986 ("The advent of the electronic age and . . . the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law."). Commentators have likened computer files to storage containers and plastic bags and suggested that requiring the police to rely on the file names is similar to requiring police to rely on a plastic bag labeled "talcum powder" or "flour." *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 207–10 (2005–06) (citing United States v. Hill, 322 F. Supp. 2d 1081, 190–91 (C.D. Cal. 2004)).

67 *See In re* Search of 3817 W. West End, Chicago, Illinois 60621, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) ("Even a modest home computer today frequently has 512 megabytes of memory (if not more), which translates into capacity of 256,000 pages of information.").

68 *See* United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005) (discussing the problems with ex ante search protocols for searching computers and noting that "[g]iven the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science").

determine whether the police lawfully seized evidence related to the warrant.[69] Others have suggested a special approach is necessary and that a judge or magistrate should become heavily involved in the scope of the warrant, describing with the utmost detail precisely which files should be searched and, to some extent, how to go about searching them.[70] These two approaches have emerged as the leading views as to how the plain view doctrine should apply in computer evidence cases.[71]

2. The Ninth Circuit's Direct "Special Approach"

In *United States v. Tamura*, the Ninth Circuit first addressed the issue of how to handle the search and seizure of intermingled physical files—a concept intimately related to computer evidence searches.[72] The court

---

[69] For the purpose of this Note, this will be referred to as the "container theory" or "container approach." Courts adhering to this approach have generally looked to traditional Fourth Amendment principles—such as probable cause and particularity—in limiting the scope of a particular search or seizure. *See* United States v. Gleich, 293 F. Supp. 2d 1082, 1088 (D.N.D. 2003), *aff'd*, 397 F.3d 608 (8th Cir. 2005) (finding that the warrant authorizing search of computer for photographs, pictures, visual representations, or videos that included sexual conduct by a minor, as defined by the state statute, met the particularity requirement and also finding that the warrant authorizing the search of the home permitted a search of all three computers in the house); United States v. Campos, 221 F.3d 1143, 1147–48 (10th Cir. 2000) (finding warrant sufficiently particular when it authorized, among other things, seizure of computer equipment that may have been used to depict or distribute child pornography); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (upholding a warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in the home of a woman suspected of child pornography (omissions in original)); United States v. Hall, 142 F.3d 988, 996–99 (7th Cir. 1998) (holding that the particularity requirement was satisfied when items listed in a warrant qualified that the items sought were related to child pornography); State v. Wible, 51 P.3d 830, 837 (Wash Ct. App. 2002) (finding that a warrant was sufficiently particular when it limited the search to images of children engaged in sexually explicit activity as defined by state statute).

[70] *See infra* Part II.B.2–3 (discussing the special approaches to the plain view exception as applied to computer evidence cases, as well as the closed-container analogy and other various theories).

[71] *See* United States v. Kim, 677 F. Supp. 2d 930, 943–49 (S.D. Tex. 2009) (recognizing that "neither the Fifth Circuit nor the United States Supreme Court have developed precedent specifically addressing the scope of a search for digital evidence," and that "the Ninth Circuit has the most robust body of law on the subject matter," and subsequently examining—in distinct and separate sections of the opinion—the approach that the Ninth and Tenth Circuits have taken to reconcile plain view analysis with digital evidence); *see also infra* Part III.B–C (discussing the positive and negative aspects of each of the approaches).

[72] 694 F.2d 591 (9th Cir. 1982). In *Tamura*, the defendant was involved in a bribery scandal and officers entered Tamura's business subject to a warrant that authorized them to find and seize various business records. *Id.* at 594. The police were permitted to seize the following: (1) records of contracts for the sale of cable during a four and one-half year period, (2) records of payments during the same four and one-half year period, and

began by noting that while all items in a set of files may be inspected during a search—provided the warrant offers sufficiently specific guidelines for identifying the relevant documents—a wholesale seizure of all relevant documents is considerably more intrusive.[73] The court (1) determined that a valid search warrant described all of the seized documents introduced at trial; (2) noted that in the future, when dealing with documents that are so intermingled they cannot feasibly be sorted on site, the government should seek the judgment of a neutral and detached magistrate; and (3) stated that the government "generally can

---

(3) records of travel for a similar time period. *Id.* When the original means of collecting data became overly burdensome, the employees of the company refused to cooperate, and the agents confiscated all of the records for the time period in question regardless of their relevance. *Id.* at 595. To find the relevant records in the accounting department, the agents had to perform three steps: (1) review a computer printout; (2) locate the voucher that corresponded to a particular payment recorded on the printout; and (3) find the check that corresponded to the voucher. *Id.* at 594–95. In all, the officials seized eleven cardboard boxes of computer printouts, which were bound in 2000-page volumes; thirty-four file drawers of vouchers, also bound in 2000-page volumes; and seventeen drawers of cancelled checks, which were bundled into files. *Id.* The agents hauled all these records to another location, where they sifted through them and extracted the relevant documents. *Id.* The defendant did not contest the validity of the search warrant; he challenged only the scope of the seizure. *Id.* Notably, when the Supreme Court addressed the issue in *Andresen v. Maryland*, the Court held that inevitably "innocuous" documents can be "cursorily" examined. 427 U.S. 463, 482 n.11 (1976). Other courts have set forth guidelines for governmental review of commingled records to find documents that fall within the scope of a warrant. *See, e.g.*, United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1982) (allowing for a "brief perusal" of each document, and requiring that "the perusal must cease at the point at which the warrant's inapplicability to each document is clear"); *see also* United States v. Rude, 88 F.3d 1538, 1551–53 (9th Cir. 1996) (suggesting that officers may "peruse each document to determine whether it relate[s] to other fraudulent activity," but finding that where it was "readily apparent" that certain documents were beyond the scope of the warrant and agents were "immediately alerted" to that fact, the Fourth Amendment was likely violated); United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990) (holding that "the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized"); United States v. Slocum, 708 F.2d 587, 604 (11th Cir. 1983) (finding government agents did not act unlawfully where they "merely examined documents . . . to determine if the documents might in some manner relate to [certain] transactions" that were described in the warrant); United States v. Ochs, 595 F.2d 1247, 1257 n.8 (2d. Cir. 1979) (holding valid government action described as "some perusal, generally fairly brief"). If a document falls outside the warrant but nonetheless is incriminating, the *Heldt* theory allows that document's "seizure" only if during that brief perusal the document's "otherwise incriminating character becomes obvious." *Heldt*, 668 F.2d at 1267.

[73] *Tamura*, 694 F.2d at 595. The court also noted that an indiscriminate seizure does not comply with the Fourth Amendment especially when files are not timely returned once segregated. *Id.* To summarize *Tamura*, the government was attempting to search for a single document hidden somewhere in many boxes of documents. *Id.* at 596. Rather than search through the boxes and seize only the one document, investigators carted off all the documents to search them off-site at a later time. *Id.* at 596–97.

avoid violating [F]ourth [A]mendment rights by sealing and holding the documents pending approval by a magistrate of a further search."[74] The Ninth Circuit ultimately enunciated a two prong analysis to solve the problem of intermingled documents: (1) the government should be allowed to seize all intermingled documents, regardless of relevance, in order to remove them from the suspect's control; and (2) the government should then be required to appear before a neutral and detached magistrate who can issue a second warrant that sets the conditions and limits of the file search.[75]

Likewise, the Ninth Circuit was also the first—and, as of the date of this Note, the only—circuit to directly consider the application of the plain view doctrine specifically in the context of computer evidence cases in *United States v. Wong*.[76] In *Wong*, a Ninth Circuit panel determined

---

[74] *Comprehensive Drug Testing II*, 513 F.3d 1085, 1107 (9th Cir. 2008) (citing *Tamura*, 694 F.2d at 595–96).

[75] *Tamura*, 694 F.2d at 591. The *Tamura* court's proposed solution to the intermingled document problem essentially had two elements. *Id*. at 596. First, officers should be allowed to seize all the intermingled documents in question—regardless of relevance—thus removing them from the defendant's control. *Id.* Then, after the initial seizure, the government should be required to go before a neutral and detached magistrate who would issue a second warrant and determine the "conditions and limitations" for inspecting the large quantities of computer data. *Id*. at 597 n.3.

[76] 334 F.3d 831 (9th Cir. 2003). In *Wong*, the defendant called police and notified them that his live-in girlfriend had been missing for several days. *Id*. at 833–34. Wong initially told police that he and Sin were married, when in fact, they were not. *Id*. Sin was pregnant at the time of her disappearance, a fact Wong did not tell police until days after he reported her missing. *Id.* Investigating officers discovered Sin's car a half-mile from Wong's home, ascertained that Wong and Sin had been fighting prior to her disappearance, found a handgun during a consensual search of Wong's home, and learned that shortly after Sin's disappearance Wong's other girlfriend and mother of his child, Jennifer, had moved into the house with Wong. *Id.* Police ultimately discovered Sin's body in Nevada with four bullet holes in it, as well as bullet casings that appeared to match the gun found in Wong's home and monopoly money marked with "NWO" and "ZOG" (letters commonly used by white supremacy groups) next to it. *Id*. at 834. Upon discovering this information, police officials presented to the magistrate judge a search warrant, affidavit, and statement of probable cause to search Wong's house, cars, and computer. *Id.* The search warrant limited the seizure to items used to commit a felony, evidence that tended to show a felony had been committed, or evidence that a particular person committed the felony, and also specified that officers would be looking for any effects containing information about the white supremacist letters or the county in Nevada where the body was found, and any other effects belonging to Sin. *Id*. The warrant issued, and the police collected many things, including the computers. *Id.* A special agent was called in to gather information from the computers; he determined that information regarding the firearms, felonies, the white supremacist letters, and the county in Nevada could be located by searching plain text, special text, or graphics files. *Id*. at 835. In particular, the specialist thought that maps of the county in Nevada, and depictions of Monopoly money and the white supremacist letters, might be found on the computer and those would likely be found in graphic files. *Id.* After the specialist began his search, he located graphic files containing child

that a search warrant was sufficiently particular and was supported by probable cause; however, as the court noted, the government still had to establish the requisite elements of the plain view doctrine.[77] Because the computer specialist determined the items listed in the search warrant could be located in plain text, special text, or graphic files on the computer, and because the police found the child pornography files while searching for evidence of the homicide, the court found that the police were lawfully present at their vantage point.[78]

The Ninth Circuit recently had a chance to refine its position as to how the plain view exception should apply in computer-based evidence cases, as well as how the intermingled documents problem might best be solved in *United States v. Comprehensive Drug Testing, Inc*.[79] In *Comprehensive Drug Testing*, the government obtained a search warrant to search the computer files of Comprehensive Drug Testing, Inc., for the names and test results of ten specified major league baseball players.[80]

---

pornography; he made note of their location and continued his search for evidence relating to the homicide. *Id*. In addition to searching the house and the car, one item on the warrant sought to search Wong's computers, their components, and disks to "obtain data as it relates to this case." *Id*. at 834. Specifically, the warrant list included any writings, documents, maps, or receipts depicting or relating to Churchill County, Nevada; and "[a]ny and all identification and documents belonging to [the murder victim]." *Id*. at 837.

77 *Id.* at 838. The Ninth Circuit panel further recognized that in order "[t]o satisfy the plain view doctrine: (1) the officer must be lawfully in the place where the seized item was in plain view; (2) the item's incriminating nature was 'immediately apparent'; and (3) the officer had 'a lawful right of access to the object itself.'" *Id.* (citing Horton v. California, 496 U.S. 128, 136–37 (1990)). The *Wong* court found that, pursuant to a valid search warrant, the officer had determined the items listed in the search warrant that could be located on computer files could be found in plain text, special text, or graphic files. *Id.* While searching the graphics files for evidence of murder, as allowed by the warrant, the officer discovered pictures of children as young as age three engaged in sexual acts. *Id.* The incriminating nature of the files was immediately apparent to the officer. *Id*. Because the police were lawfully searching for evidence of murder in the graphics files and inadvertently located the incriminating child pornography, the evidence was properly admitted under the plain view doctrine. *Id*. at 838–39.

78 *Id.* The court also found that the incriminating nature of the files was immediately apparent to the specialist since they depicted children as young as three engaged in sexual acts; therefore, the court concluded that the evidence was properly admitted under the plain view doctrine. *Id*. at 839.

79 *Comprehensive Drug Testing III*, 579 F.3d 989 (9th Cir. 2009) (en banc), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc).

80 *Id.* at 993–94. The warrant had an introduction that painstakingly chronicled the need for the government to search all of the files because of the tendency of wrongdoers to attempt to disguise and hide files, or even set up booby-traps that will destroy the information if triggered. *Id*. at 1002. Therefore, the government claimed they needed to sift through each of the files independently and prudently. *Id.* at 1003–06. The court aptly recognized, however, that this will be the case in all digital and computer evidence cases, and held that in the future the government must disclose the *actual* possibility of these dangers as opposed to the ever-present danger in the abstract. *Id.* at 1006. Many of the

During the search of the computers, the government arguably violated certain terms of the search warrant by "perus[ing]" through all of the computer files of the company without regard for whether the files pertained to the ten specified players.[81] The government argued that it complied with the standard set forth in *Tamura*, but it was not required to return the additional evidence because it was obtained "in plain view."[82]

The Ninth Circuit, sitting en banc, found that the government acted with callous disregard for the warrant requirements issued by the magistrate by browsing all of the computers files and set out a series of guidelines that should be used in subsequent digital evidence cases.[83] The en banc court reasoned that *Tamura* imported procedures to maintain "privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search . . . into a general search."[84] The court suggested that warrants should contain language or

---

judges in the lower courts of this case indicated that they felt exceedingly misled by the government's actions. *Id.* at 1005–06. For instance, one of the judges issuing a warrant asked "what ever happened to the Fourth Amendment? Was it . . . repealed somehow?" *Id.* at 1005.

[81] *Id.* at 999. The Major League Baseball Players Association agreed that players would submit urine samples solely for determining the percentage of positive results; all results were to remain confidential. *Id.* But when ten players tested positive, the government obtained warrants and issued subpoenas to obtain information from private entities who collected the samples and information. *Id.* at 997. The warrants were limited to information on the ten players, but the government seized information on many others, including athletes from other professional sports. *Id.* at 998. The government also issued subpoenas for the same information. *Id.* The lower courts granted the players' motions to quash and to return seized property. *Id.* The Ninth Circuit, sitting en banc, determined that the government was not able to rely on the plain view doctrine or any similar doctrine to justify the seizure of the information. *Id.* at 999.

[82] *Id.* at 997. A panel of the Ninth Circuit decided the case initially and ruled that the government lawfully obtained the evidence pursuant to the warrant; this opinion was subsequently withdrawn and superseded by a second panel decision that concluded ultimately the same.

[83] *See id.* at 1006 (providing a synopsis of the guidelines that the court employs during the course of its decision).

[84] *Id.* at 998. The court further suggested that if the government cannot be sure whether data can be erased, concealed, or destroyed without examining every file, then every file the government comes into contact with will necessarily come into plain view. *Id.* Additionally, if the government is the entity that decides how much evidence will be taken from the site, it creates a powerful incentive for the government to overestimate the amount of evidence needed or simply lead to a seizure of "more rather than less." *Id.* The court illustrated the possible thought process aptly with the following hypothetical excerpt:

> Why stop at the list of all baseball players when you can seize the entire . . . Directory? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been.

protocol that prevents over-seizure of data, such as employing separate search personnel trained specifically with computers or using specialized hashing equipment.[85] And perhaps most notably, the court further mandated that when the government obtains search warrants, it should forswear use of the "plain view" doctrine in electronic evidence cases; if the government refuses to do so, district courts should require it or deny the warrant altogether.[86]

The Ninth Circuit concluded by recognizing that wrongdoers "have obvious incentives to make data difficult to find" and that the government has a legitimate need to sift through some information carefully for disguised pieces of evidence, but that such a pressing need by law enforcement cannot justify every search warrant for computer evidence becoming, in effect, a general warrant to search every piece of information therein.[87] The court attempted to create clear rules that

---

> Let's take everything back to the lab, have a good look around and see what we might stumble upon.

Id. (citation omitted).

[85] *Id.* at 996. The court suggested that the personnel could either be employed through the police force or government, or they could be privately contracted. *Id.* The court also suggested that in certain cases, the personnel to sort the files should be appointed by the judicial officer in charge of issuing the warrant. *Id*. In December 2009, for instance, a district court within the Ninth Circuit determined that the search protocol provided by the warrant—including that the government could only remove an electronic device from the search location if it could not be searched reasonably on-site and that the government had to complete an off-site search no later than thirty calendar days after the initial execution of the warrant and had to return the device within thirty calendar days after the search. United States v. Cerna, No. CR 08-0730, 2009 U.S. Dist. LEXIS 122847, at *24 (N.D. Cal. Dec. 21, 2009). The protocol also required the government to make "all reasonable efforts" to use methods and procedures that minimized exposure of irrelevant, privileged, or confidential files. *Id*. The district court concluded that the protocol "was sufficiently tailored to meet the criteria established in *Comprehensive Drug Testing*." *Id*.

[86] *Comprehensive Drug Testing III,* 579 F.3d. at 998–99. The majority and dissenting opinions quarreled over the relevance of the "plain view" doctrine in such cases and whether allowing the doctrine created a free-for-all of "general" searches when computers are involved. *See id.* (suggesting that if the government can apply the plain view doctrine in the context of digital searches and seizures it effectively risks the privacy of the entire American populace). "To avoid this illogical result," the majority opinion also suggested that the government should forswear reliance on "any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data." *Id. But see* United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 (D. Me. Dec. 3, 2009) (suggesting that the Ninth Circuit approach is perhaps misguided because it presumes police misconduct is the rule, rather than the exception).

[87] *Comprehensive Drug Testing III*, 579 F.3d at 1004 The court was clearly taken aback by the actions of the government and wondered what the bounds might be in the future, noting that authorization to search some computer files, by virtue of the government's reliance on the plain view exception, automatically becomes authorization to search all of the files "in the same subdirectory, and all files in an enveloping directory, a neighboring

struck a fair balance between individual and law enforcement interests, and felt the need "to update *Tamura* to apply to the daunting realities of electronic searches."[88]

After the court issued its original en banc decision in *Comprehensive Drug Testing*, several parties to the litigation, including the Department of Justice ("DOJ"), requested that the Ninth Circuit rehear the case by a "Full Court."[89] The Ninth Circuit ultimately denied the requests for rehearing en banc by the full court[90] and instead opted to issue a per curiam opinion that would revise and supersede the original en banc

---

hard drive, a nearby computer or nearby storage media." *Id.* at 1005. And where computers happen not to be near one another, but are connected electronically, "the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there." *Id.* Concerning the majority even more is perhaps the development of web-based e-mail accounts, picture sharing sites, slideshows, computer codes, etc., that store messages, pictures, or other data "along with billions of other messages from and to millions of other people." *Id.* Therefore, the court concluded that under the government's formulation of the plain view exception, seizure of Google's e-mail servers "to look for a few incriminating messages could jeopardize the privacy of millions." *Id.*

88 *Id.* at 1006. On the other hand, courts adhering to the closed container approach to computers—or at least those opting to insist on adherence to the common law approach of reasoned decisionmaking based solely on the facts at hand—have simply applied existing Fourth Amendment doctrine to the searches of computers. *See, e.g.*, United States v. Riccardi, 405 F.3d 852, 863 (10th Cir. 2005) (holding that a warrant that "permitted the officers to search for anything—from child pornography to tax returns to private correspondence," was "precisely the kind of 'wide-ranging exploratory search[] that the Framers intended to prohibit'" (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987))); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) ("[O]fficers [should] specify in a warrant which type of files are sought."); United States v. Hunter, 13 F. Supp. 2d 574, 584–85 (D. Vt. 1998) (invalidating a warrant for failure to identify with particularity the underlying information to be seized); *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (holding in the context of a grand jury subpoena that specificity is required with respect to the categories of information requested, not merely the storage devices).

89 *See* Orin Kerr, *DOJ Files Brief Supporting Super-En-Banc in CDT*, VOLOKH CONSPIRACY (Nov. 24, 2009, 1:26 PM), http://volokh.com/2009/11/24/doj-files-brief-supporting-super-en-banc-in-cdt. The brief filed on behalf of the Justice Department—signed by many of the highest ranking attorneys in the DOJ—criticized the original en banc panel for having articulated such "sweeping new rules," noted that the government had never asked for—and the Ninth Circuit had never granted—en banc review by the full court, and ultimately sought rescission of the original opinion or, alternatively, a chance to brief the court on the repercussions of the new protocol. *See id.*

90 *See* Musetta Durkee, *Ninth Circuit Relaxes Electronic Search Procedures in* United States v. Comprehensive Drug Testing *Rehearing*, BOLT (Sept. 28, 2010), http://btlj.org/2010/09/28/ninth-circuit-relaxes-electronic-search-procedures-in-united-states-v-comprehensive-drug-testing-rehearing ("Following . . . requests from Solicitor General Kagan and others on behalf of the Obama Administration, the Ninth Circuit conceded to revisit the opinion en banc, but denied the super en banc request.").

decision.[91] In response to pressures by law enforcement officials—not to mention the Obama administration and then-Solicitor General Elena Kagan—the Ninth Circuit's revised opinion employs much of the same language as the original en banc decision, but relaxes the mandatory procedures for issuance of a warrant by omitting the language exacting mandatory requirements on government officials.[92] Chief Judge Kozinski—the author of the original en banc majority opinion—issued a concurring opinion joined by four other judges, which recited precisely the same limitations on government as the original en banc decision, and continued to urge magistrate judges to require the government to "forswear reliance on the plain view doctrine."[93] The immediate effect of

---

[91] *See Comprehensive Drug Testing IV*, 621 F.3d 1162, 1165 (9th Cir. 2010) (en banc) (per curiam) (ordering the revision of the original en banc decision and denoting that the new en banc decision shall "constitute the final action of the court"). Notably, the new decision by the Ninth Circuit is no longer attributed to Chief Judge Kozinski, who instead filed a concurring opinion. *See id.* (revising and superseding the original en banc decision penned by Chief Judge Kozinski); *Comprehensive Drug Testing III*, 579 F.3d at 993 (constituting the original en banc disposition authored by Chief Judge Kozinski).

[92] *See* Durkee, *supra* note 90 ("Federal prosecutors and the Obama administration contested that these procedural requirements were too stringent. . . . [T]hen-Solicitor General Elena Kagan argued that the Ninth Circuit's strict guidelines produced a 'chill[ing]' effect on the ability of prosecutors to obtain new search warrants for computers and other electronic data and records." (second alteration in original)). *Compare Comprehensive Drug Testing III*, 579 F.3d at 1006 (recounting the protocol government should follow in seeking warrants), *with Comprehensive Drug Testing IV*, 621 F.3d at 1177 (employing precisely the same language as the original en banc majority opinion by Kozinski, C.J., but omitting the controversial recitation of limitations on the government in the "Concluding Thoughts" section of the opinion).

[93] *Comprehensive Drug Testing III*, 579 F.3d at 998. *Compare id.* at 1006 (enunciating five limitations on government in the context of searches and seizures of electronically stored information), *with Comprehensive Drug Testing IV*, 621 F.3d at 1179 (Kozinski, C.J., concurring, joined by Kleinfeld, Fletcher, Paez, and Smith, JJ.) (enunciating the same five limitations on government and reiterating that "[i]f the government believes it's entitled to retain data as to which no probable cause was shown in the original warrant, it may seek a new warrant or justify the warrantless seizure by some means other than plain view"). Chief Judge Kozinski also reaffirmed his belief that

> [w]hen the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium . . . or when a search for evidence could result in the seizure of a computer, magistrate judges should insist that the government forswear reliance on the plain view doctrine[, and] should also require the government to forswear reliance on any similar doctrine that would allow retention of data obtained only because the government was required to segregate seizable from non-seizable data. This will ensure that future searches of electronic records do not "make a mockery of *Tamura*"—indeed, the Fourth Amendment—by turning all warrants for digital data into general warrants. If the government doesn't consent to such a waiver, the magistrate judge should [require separation] by an independent third party . . . or deny the warrant altogether.

the Ninth Circuit's revision is that the five limitations announced by the court in the original en banc decision are no longer binding authority, but now merely provide guidance to magistrates in attempting to balance the Fourth Amendment's mandates with law enforcement's needs in effective and efficient operation.[94] Although the Ninth Circuit amended its position as to the plain view doctrine's application to digital searches and seizures to permit the government more latitude, the volatile disposition of the case, and the circuit's inability to issue a decision with which it was satisfied, serve to highlight the daunting tasks that face magistrates and appeals courts alike in attempting to fashion constitutional rules that adequately serve each of the competing interests.[95]

3. The Tenth Circuit's Indirect "Special Approach"

In *United States v. Carey*, the Tenth Circuit addressed the similar issue of whether a police search was constitutional under the Fourth Amendment and created a "special approach" to digital evidence cases.[96] In *Carey*, a law enforcement official searching a computer pursuant to a warrant for evidence relating to narcotics came across images of child pornography.[97] He subsequently abandoned the search for the narcotics evidence named in the warrant and began to look for additional images of child pornography.[98] The Tenth Circuit concluded that the search for

---

Id. at 1178 (citation omitted).

94 *See Comprehensive Drug Testing IV*, 621 F.3d at 1183 (Callahan, J, concurring in part and dissenting in part) ("I initially express my concerns with the proposed guidelines for searches of electronically stored data that are set forth in the Chief Judge's concurring opinion. The concurrence is not joined by a majority of the en banc panel and accordingly the suggested guidelines are not Ninth Circuit law."); Durkee, *supra* note 90 ("In practical effect, this revised en banc opinion no longer makes Kozinski's five-part procedural requirements binding for magistrate courts. Instead, magistrate[s] are required only to use these five procedural safeguards as 'a useful tool for the future.'" (quoting *Comprehensive Drug Testing IV*, 621 F.3d at 1180 (Kozinski, C.J., concurring))).

95 *See Comprehensive Drug Testing IV*, 621 F.3d at 1177 (majority opinion) ("[The reality that over-seizing is inherent within the digital search context] calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."). The new decision ultimately recognized that "[e]veryone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment," and "updated *Tamura* to apply to the daunting realities of electronic searches." *Id*.

96 172 F.3d 1268, 1271, 1275 n.7 (10th Cir. 1999).

97 *Id.* at 1271.

98 *Id*. The defendant had been under investigation for possible sale and possession of cocaine, and the police obtained a warrant for his arrest. *Id*. While at his residence,

additional images was improper and employed a "special approach" in an attempt to avoid allowing discovery of evidence outside the scope of the warrant in computer searches.[99]

The defendant argued that the search of the computers transformed the warrant into a "general warrant" and resulted in a general—and therefore illegal—search of the computers and their files.[100] The government alleged that the plain view doctrine authorized the police seizure of the files and that the defendant's written consent allowed their

---

however, the police noticed in plain view a bong and what appeared to be marijuana; surprised, the police asked for consent to search the rest of the apartment, and after much discussion, Carey obliged and signed a formal written consent. *Id*. With such consent, the officers returned to the apartment later that night and discovered cocaine, marijuana, and hallucinogenic mushrooms. *Id*. The officers also seized two computers that they believed might evidence drug dealing, which they took back to the police station and obtained a warrant to search. *Id.* at 1272. The warrant allowed the police to search for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." *Id*. at 1272–73. The police copied the hard drives and began searching through the files by entering key words into the computer's search mechanism to find "text-based" files containing such words; this search, however, produced no files "related to drugs." *Id*. at 1271. The key words were terms such as "money, accounts, people, so forth." *Id.* The officers continued their search by sifting through the directories until they encountered some files they "[were] not familiar with," which were non-text, JPG files. *Id*. An officer opened the first file and it contained child pornography. *Id*. The police copied the rest of the JPG files to disks and searched through approximately one hundred more in attempting to locate additional evidence of child pornography. *Id.* When being questioned by the government, the officer searching the computer files stated that until he opened each file, he really did not know its contents. *Id*. However, he acknowledged that he downloaded and viewed these files knowing each of them contained pictures. *Id*. Still, he claimed that "I wasn't conducting a search for child pornography, [but] that happened to be what these turned out to be." *Id*. From the tone of the opinion, the court seemed hesitant to believe his testimony. *See id.*

[99] *Id*. at 1275 n.7, 1277. The court advised: "Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." *Id.* at 1275. This special approach has gained much headway in the judiciary, but also has many skeptics. *See* RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 49 (2007) (suggesting that much of the problem with the Tenth Circuit's approach in *Carey* was the unwillingness of the court to directly apply the plain view doctrine to digital evidence); *infra* Part III.B (discussing the pros and cons of applying a special approach to the application of the plain view doctrine to computer-related evidence).

[100] *Carey*, 172 F.3d at 1271–72. The defendant in *Carey* argued that, when examined against the history and case law of the Fourth Amendment, the search constituted general rummaging in "flagrant disregard" for the terms of the warrant and in violation of the Fourth Amendment, and that despite the specificity of the search warrant, files not pertaining to the sale or distribution of controlled substances were opened and searched, and such files should have been suppressed. *Id*. at 1272.

search.[101] The Tenth Circuit found the government's plain view argument unavailing because the investigator had to open the files to view them before he knew whether they contained drug-related activity.[102] The court reasoned that because the warrant permitted only the search of the computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances," the scope of the search was limited to evidence relevant to drug trafficking.[103] The court noted that when the investigator discovered the first pornographic image he abandoned his search for drugs and began searching for similar pornographic materials and thus was searching outside the parameters of the warrant.[104] The court resolved the case on other grounds,

---

[101] *Id.* According to the government's line of argument, "a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography." *Id.* The government's reasoning continued that "[j]ust as if officers ha[d] seized pornographic photographs from a file cabinet, seizure of the pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent." *Id.* The warrant, therefore, "authorized the officer to search any file because 'any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information.'" *Id.* Finally, the government argued that the defendant's consent to search the apartment overrode all of these questions because it extended to the search of every file on both computers. *Id.*

[102] *Id.* at 1273. The court aptly stated that "it is the contents of the files and not the files themselves which were seized," and noted that the investigator "could not at first distinguish between the text files and the JPG files upon which he did an unsuccessful word search. Indeed, he had to open the first JPG file and examine its contents to determine what the file contained." *Id.* Thus, the court analogized the files on the computer with separate compartments in a coat or suitcase; each must be opened individually and the contents examined before the police will know what each contains. *Id.* at 1277.

[103] *Id.* at 1272–73. The Tenth Circuit ultimately looked to the subjective intent of the officer conducting the search and seizure. *See id.* at 1273 (noting that the officer "abandoned [his original] search" by looking at the subsequent files, and, thus, because the officer "expected to find child pornography and not material related to drugs," the court was unable to say "the contents of each of [the subsequent] files were inadvertently discovered"). Interestingly, the Supreme Court has explicitly concluded that whether evidence is discovered inadvertently is completely irrelevant to the Fourth Amendment analysis in regards to the plain view doctrine—at least insofar as physical evidence is concerned. *See* Horton v. California, 496 U.S. 128, 138–40 (1990) (concluding that the "inadvertence requirement" of the plain view doctrine should no longer be analyzed as part of the application of the doctrine).

[104] *Carey*, 172 F.3d at 1277 (Baldock, J., concurring). After viewing the contents of the first file, the investigator, according to his own testimony, stated that he then had "probable cause" to believe the remaining JPG files contained similar erotic material. *Id.* at 1276. Thus, through the investigator's own admission, it was clear that each time he opened a

ultimately concluding that all but the first pornographic image were outside the scope of the warrant, but noted in dicta that the pornographic images were in closed files and thus not in plain view.[105] The court also provided several means by which investigators could tailor their future conduct to meet the commands of the Fourth Amendment: they could observe file types and titles listed on the directory, do a key word search for relevant terms, or read portions of each file stored in the memory.[106]

One enduring aspect of the Tenth Circuit's opinion in *Carey* is the court's rejection of the government's proposed "file cabinet" analogy, and its realization that computers are likely to contain large quantities of intermingled documents.[107] The Tenth Circuit concluded that file cabinet

---

subsequent JPG file he expected to find child pornography and not material related to drugs. *Id*.

[105] *Id*. at 1273 (majority opinion). The court noted that "[a]lthough the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here." *Id*. The Tenth Circuit ultimately determined that the fact the files were labeled as "JPG" and had sexually suggestive titles, the officer knew—especially after opening the first of the pornographic files—that he was not going to find drug related activity. *Id*. at 1274.

[106] *Id.* at 1276.

[107] *Id.* at 1275. Academics have likewise supported this notion. *See* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 60–63, 81–82 (2002), *available at* http://www.mttlr.org/voleight/Brenner.pdf (suggesting that computers and computer storage systems differ from paper documents, and therefore require different rules and approaches). Many courts, however, have also analogized computers to other more familiar tangible objects such as datebooks, containers, briefcases, and other closed containers. *See*, *e.g.*, United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993). In *Chan*, the court stated that "[t]he expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information." *Id.* Courts have also held that "an individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as in a closed container." *Id.* at 535 (quoting United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990)); *see also* United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (holding that a computer's memory, due to its ability to store and hold large amounts of information, "is indistinguishable from any other closed container, and is entitled to the same Fourth Amendment protection" (citing Robbins v. California, 453 U.S. 420, 427 (1981))). Although appellate courts have upheld some searches and seizures of computer memory devices, these courts have all relied on an individual's lack of standing to challenge the search and have avoided indications that computer memory enjoys anything other than a very high level of protection. *E.g.*, United States v. Lyons, 992 F.2d 1029, 1031–32 (10th Cir. 1993); United States v. Meriwether, 917 F.2d 955, 958–59 (6th Cir. 1990). Further, the Department of Justice relies, at least in part, on the closed container approach to digital searches and seizures. *See generally* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS pt. I.B.2 (July 2002), *available at* http://purl.access.gpo.gov/GPO/LPS36377 ("To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such

and closed-container analogies to computers and computer files are insufficient because they oversimplify the realities of mass storage devices.[108] The Fourth Amendment should provide protection in an area that was little contemplated during its proliferation.[109]

III. ANALYSIS

Courts have certainly struggled in attempting to apply traditional rules and concepts of Fourth Amendment jurisprudence in the context of computer and digital evidence. Part III of this Note discusses the positive and negative aspects of the various approaches courts have taken in an attempt to reconcile these novel difficulties with the Fourth Amendment's constitutional protections.[110] Part III.A specifically discusses the circumstances under which computer searches become overly broad and the avenues courts have employed to combat this phenomenon.[111] Part III.B analyzes the "special approaches" that courts have taken in an attempt to reconcile Fourth Amendment jurisprudence, individual civil liberties, and the government's interest in the proper administration of justice, and discusses both the helpful and problematic facets of the judicial attempts.[112] Finally, Part III.C evaluates the ability of the container analogy to adequately safeguard constitutional rights, while remaining sympathetic to the efforts of law enforcement.[113] Ultimately, Part III concludes that existing approaches fail to properly

---

as a briefcase or file cabinet," and that the Constitution generally does not allow for the government "accessing and viewing information stored in a computer . . . if it would be prohibited from opening a closed container and examining its contents in the same situation").

108 *Carey*, 172 F.3d at 1275. Computer storage is likely to contain a greater quantity and variety of information than storage methods from the past and as a result "computers make tempting targets in searches for incriminating information." *Id.* (quoting Winick, *supra* note 14, at 104). "Relying on [such misplaced analogies] may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'" *Id.* (quoting Winick, *supra* note 14, at 110).

109 *See infra* Part III.B–C (discussing the positive and negative aspects of the different approaches courts have taken to attempt to abide by this concept).

110 *See infra* Part III (analyzing the approaches courts have taken when applying the plain view doctrine in the context of digital evidence cases).

111 *See infra* Part III.A (discussing the circumstances under which warrants may become general and the attempts by courts to reconcile what they discern to be a novel dilemma within Fourth Amendment jurisprudence).

112 *See infra* Part III.B (analyzing the "special approaches" that courts have taken to attempt to solve this problem, and the positive and negative aspects of this line of reasoning).

113 *See infra* Part III.C (evaluating the feasibility of the closed-container analogies between computers and containers in the ambit of Fourth Amendment jurisprudence, and more specifically, in regard to the plain view doctrine).

balance the competing interests involved in computer evidence cases and discusses the shortcomings of the various approaches to the problem while leaving open possible solutions and avenues for remedy.[114]

A. When Computer Searches Become General

Why should it matter that the government is able to sift through all of the files on a given computer? And should information stored on a computer system or general server be afforded more or less constitutional protection under the Fourth Amendment? It is generally accepted that if, in the context of digital evidence, police are otherwise in a valid position to view the computer screen, the images on the screen will be deemed in "plain view."[115] However, courts and scholars dealing with the more complicated issue of data stored within a computer—or even data on an entire computer system—have created two independent lines of reasoning, each with its own advantages and disadvantages.[116]

---

[114] *See infra* Part IV (proposing a solution to the problem of applying the plain view doctrine in the context of computer evidence cases).

[115] *Compare* People v. Blair, 748 N.E.2d 318, 323 (Ill. App. Ct. 2001) (holding that police who observed "bookmarks with references to teenagers and so forth," did not have probable cause to believe that computer contained child pornography), State v. Mays, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (holding that observations of a computer screen during the search of a home qualified as in plain view), *and* State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604–05 (Okla. Civ. App. 1995) (during execution of search warrant based on allegations that suspect was distributing pornographic material, police observations of computer established that the equipment and its possible criminal use were in plain view), *with* United States v. Turner, 169 F.3d 84, 88 (1st Cir. 1999) (holding that the observation of nude women on computer screen by officer during search of apartment did not justify search of computer for other incriminating data), *and* State v. Brown, 813 N.E.2d 956, 960–62 (Ohio Ct. App. 2004) (holding that the incriminating nature of computers and their contents is not immediately apparent based on mere observation of two computers in defendant's house, where there was no pornography displayed on screen, and where police merely knew that pornographic material had been printed from a computer).

[116] *See Comprehensive Drug Testing III*, 579 F.3d 989, 997–98, 999, 1000–01, 1003–04, 1006 (9th Cir. 2009) (en banc), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (creating a special approach and establishing guidelines that should be "vigilant[ly]" adhered to by lower courts). These guidelines are as follows:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction [of computer data] must be either done by specialized personnel or an independent third party. . . .
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

The first view suggests that digital evidence searches require a special approach—even going as far as to forswear use of the plain view doctrine entirely and provide judicially imposed guidelines for executing a search.[117] This approach is impractical as applied, stifles the administration of justice, and finds little if any foundation in

---

> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006. *Compare id.* (urging magistrates to require the government to forswear reliance on either the plain view doctrine or any other similar doctrine), *with* United States v. Giberson, 527 F.3d 882, 890–91 (9th Cir. 2008) (holding that the government's discovery of child pornography was inadvertent during a search for fake ID's and therefore valid pursuant to the plain view exception), *and* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (suggesting that the correct inquiry asks whether the official "abandoned" his original search and therefore unconstitutionally expanded the scope of the warrant—turning the initially limited and constitutional search into a general, exploratory, and unconstitutional search).

[117] *See, e.g.*, *Carey*, 172 F.3d at 1272–75 (holding that continuing to open files in a search for child pornography after the first file had already been opened and observed, during the execution of a search warrant for documentary evidence relating to drugs, could not be justified by the plain view doctrine because the files were "closed" and unambiguously labeled). The Tenth Circuit in *Carey* further suggested that the search of the computer was limited by judicial discretion including, for example, searches by file name or file type. *Id.* at 1273. Interestingly, however, both the Ninth and Tenth Circuits—as well as a number of other courts—have explicitly found that search protocols are not necessary because the object of the search serves to narrow the search itself. United States v. Hill, 459 F.3d 966 (9th Cir. 2006); United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005). That is to say, if agents are issued a warrant to search for files related to child pornography, the fact they are authorized to look only for child pornography is enough to keep the search within the scope of the warrant. *See Hill*, 459 F.3d at 970–71 (suggesting that the object of the search can serve to narrow the scope of the search); *Brooks*, 427 F.3d at 1253–55 (suggesting the same). Suppose, however, that the government has probable cause to believe an individual is going to launch a terrorist attack on a given landmark or well-known area. Under a special approach, the government might be prohibited from immediately reviewing the entire contents of a computer to ascertain whether other terrorist schemes were being plotted against other areas in the United States. *See Comprehensive Drug Testing III*, 579 F.3d at 998 (imposing strict judicial guidelines that forswear the plain-view doctrine or any similar doctrine in computer evidence cases); *Carey*, 172 F.3d at 1268 (imposing a special approach that inquires as to the subjective intent of the officer to be used in computer evidence cases). *But see Giberson*, 527 F.3d at 887–88 (declining to impose heightened Fourth Amendment protections in computer search cases unless they are "based on a principle that is not technology-specific"). To see how this Note's proposed solution would handle such a dilemma, see *infra* Part IV.B.1 (suggesting that if the government knew of the additional threats prior to executing the warrant and failed to particularize them therein—either negligently or because it was unsure as to whether probable cause existed—the seizure would be unconstitutional; otherwise, the government would be allowed to conduct their search within the scope of the warrant and seize any information regarding the additional plots).

precedent.[118] This view not only generates substantial costs to society and underestimates the guile of modern criminals in their ability to conceal digital information with rapidly increasing ease, but disregards the Supreme Court's holding in *Horton v. California*, which completely dispelled the inadvertence requirement to plain view seizures.[119]

The second view equates computers with closed containers, such as lockers, briefcases, and luggage, and the data stored therein as contents of the container.[120] This view, to some extent, underestimates the differences between digital evidence and physical evidence and grants great latitude to the government in executing search warrants.[121] Nonetheless, it finds foundation in Fourth Amendment precedent and provides for adequate enforcement of the law.[122] Ultimately, these two views conflict as to the importance of the expectations of privacy in computer data, the feasibility of employing judicially crafted mandates for executions of search warrants, and the application of the Fourth

---

[118] *See* Chang, *supra* note 99, at 49 (finding that the Tenth Circuit's special approach "overlooked" clear instruction from the Supreme Court); Ziff, *supra* note 60, at 853 (suggesting that the Tenth Circuit's special approach "incorrectly relies on the subjective intent of the searching officer to determine the constitutional limits on the scope of a computer search"); *see also infra* Part III.B (discussing the positive and negative aspects of the "special approaches" to computer evidence).

[119] *See* Horton v. California, 496 U.S. 128, 138–40 (1990) (rejecting inadvertent discovery as necessary for the plain view exception but recognizing that the possibility of officers using plain view to execute pretextual searches is a legitimate Fourth Amendment concern); *see also* United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (rejecting defendant's argument that the search warrant was overbroad for failing to articulate a strategy for searching his computer and articulating that such a strategy was impracticable because defendant could have easily hidden the contraband under misleading file names).

[120] *See, e.g.*, *supra* note 88 (providing examples of courts that have required the government to identify the specific data on a computer that is sought under the warrant).

[121] *See Comprehensive Drug Testing I*, 473 F.3d 915 (9th Cir. 2006) (finding that analogies between closed containers and computers are tenuous and allows excessive government latitude in conducting searches and seizures), *vacated as moot*, 513 F.3d 1085 (9th Cir. 2008), *vacated and granted rehearing en banc*, 579 F.3d 989 (9th Cir. 2009); *see also Carey*, 172 F.3d at 1273–74 (confronting a search through defendant's computer for drug-related evidence that ultimately yielded child pornography); United States v. Turner, 169 F.3d 84, 86 (1st Cir. 1999) (confronting a search through a computer for assault-based evidence that ultimately yielded child pornography); United States v. Gray, 78 F. Supp. 2d 524, 526–27 (E.D. Va. 1999) (confronting a search through a computer for hacking-related evidence that ultimately yielded child pornography).

[122] As one court has noted, the particularity requirement of the Fourth Amendment "serves three related purposes: preventing general searches, preventing the seizure of objects upon the mistaken assumption that they fall within the magistrate's authorization, and preventing the issuance of warrants without a substantial factual basis." United States v. Vilar, No. S308CR621KMK, 2007 WL 1075041, at *21 (S.D.N.Y. 2007) (quoting United States v. Young, 745 F.2d 733, 758–59 (2d Cir. 1984)).

Amendment's particularity requirement.[123] The proper approach balances the government's interest in the administration of justice and the individual's interest in remaining free from unreasonable searches and seizures while adhering to the Supreme Court's precedential values in the realm of Fourth Amendment jurisprudence.[124]

B. The Especially Impractical "Special Approach"

As evidenced, there is relatively little case law regarding precisely how the plain view exception to the warrant requirement should apply in computer evidence cases; some scholars suggest that courts should apply the Fourth Amendment's protections zealously and absolutely.[125] Computers, as storehouses of personal information, should enjoy a strong amount of protection under the Fourth Amendment; thus, the plethora of information and ever-increasing storage capacities of home computers justifies the highest expectation of privacy.[126] Recently, a federal district court in New York explicitly embraced the file cabinet analogy as opposed to the closed-container analogy.[127] The court in *In re Grand Jury Subpoena Duces Tecum* quashed a grand jury subpoena for a

---

123 *Compare Comprehensive Drug Testing III*, 579 F.3d 989, 1012 (9th Cir. 2009) (en banc) (Callahan and Ikuta, JJ., concurring in part and dissenting in part) (expressing "several concerns regarding the breadth of the majority's new guidelines that purport to govern future digital evidence cases"), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc), United States v. Giberson, 527 F.3d 882 (9th Cir. 2008) (holding that the government search was valid because it did not proceed with its search until after an additional warrant had been obtained), *and Comprehensive Drug Testing I*, 473 F.3d at 935 ("We reject the dissent's view that government officials should limit their computer searches to key words suggested by a searched party."), *with Comprehensive Drug Testing I*, 473 F.3d at 964–65 (9th Cir. 2006) (Thomas, J., concurring and dissenting) (noting that "[t]he more sensible theory with respect to electronic data is to . . . require that a neutral magistrate examine the co-mingled data . . . to make sure that private information that the government is not authorized to see remains private. Agents who expect to encounter intermingled data or who unexpectedly encounter it may not review the data unabated, but must seek a magistrate's guidance on how to proceed"), *and* United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006) (noting that not allowing the police to seize the intermingled data for further processing would "not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive").

124 *See infra* Part IV (proposing a solution to the problem of applying the plain view doctrine in the context of digital and computer evidence cases).

125 *See, e.g.*, Kerr, *supra* note 65, at 280 (arguing that new dynamics of computer crime should result in the creation of new doctrines that "impose some new restrictions on police conduct").

126 *See* Winick, *supra* note 14 (suggesting that because computers store such a massive amount of information of various forms they are inherently entitled to heightened protection under the Fourth Amendment).

127 *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12–13 (S.D.N.Y. 1994) (applying Second Circuit case law regarding files and filing cabinets to computers and electronic documents).

company's hard disk drive because of the innate risk of exposing highly personal information.[128] Thus, it comes as no surprise that seizures of computers and digital data have inherently high potential for overreaching and intrusion.[129]

Accordingly, proponents of the special approach suggest that analogizing computers to closed containers—thus allowing extremely broad searches—relies on a "simplistic and inappropriate" characterization of computers.[130] This view suggests the fundamental differences between digitally stored data and physical data require a different analysis under the Fourth Amendment, and suggest that applying the plain view doctrine goes too far.[131] For instance, computer searches are different from physical document searches because computer forensics tools allow for more narrowly tailored searches than are possible with paper documentation.[132] However, in a reality that

---

[128] *Id.* at 13. The court further noted that although the disks might contain incriminating information, they also contained highly personal files, such as a draft of a will and personal financial information. *Id.*

[129] *See supra* note 87 (explaining that a search of digital data raises an inherent danger that the search may involve third-party data as well).

[130] *See* Winick, *supra* note 14, at 110 ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."); *see also* Brenner & Frederiksen, *supra* note 107, at 81–82 (setting forth some of the differences between searches of "paper documents and computer-generated evidence" and maintaining that courts should impose restrictions on computer searches such as limiting the search by file types by requiring a second warrant for intermingled files and imposing time frames for conducting the search). However, the Supreme Court has heard this argument and considered it unpersuasive in the past. *See generally* Horton v. California, 496 U.S. 128, 139–40 (1990) (arguing that the interest in "prevent[ing] the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements that no warrant issue unless it 'particularly describ[es] the place to be searched and the persons or things to be seized,'" and "[s]crupulous adherence to these requirements serves the interests in limiting the area and duration of the search" (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987))).

[131] *See* United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) ("We have stated our belief that the storage capacity of computers requires a special approach, and we do not intend to comment on the particularity requirement as it applies to all contemporary media."); *see also* People v. Gall, 30 P.3d 145, 160 (Colo. 2001) (Martinez, J., dissenting) ("Because computers process personal information and effects, they require heightened protection under the Fourth Amendment against unreasonable searches or seizures." (citing Winick, *supra* note 14, at 80–83)).

[132] *See In re* Search of 3817 W. West End, Chicago, Illinois 60621, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) (recognizing that "while computers present the possibility of confronting far greater volumes of documents than are typically presented in a paper document search, computers also present the tools to refine searches in ways that cannot be done with hard copy files"). However, this line of reasoning fails to account for the ingenuity of the modern criminal, and the ease with which inculpating information may be hidden, altered, or destroyed. *See* United States v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (noting that

recognizes the rapidly evolving criminal mind, many of these search processes provide a grossly inadequate means for searching for altered or encrypted file names or extensions.[133] Because there is often no way to know what is in a file without examining its contents, attempting to provide judicial direction to searches and seizures of computer data, especially prior to the search or seizure, subjects magistrates to the impracticable task of outlining methods or means by which law enforcement officials may conduct a search.[134]

This special approach further calls for a significantly circumscribed ability for law enforcement officials to search throughout an entire computer and disguises this exacting cost on the administration of justice as necessary to ensure citizens' Fourth Amendment rights.[135] Thus, when an officer comes across evidence of a crime unrelated to the given warrant, this view requires officers to completely halt the search and petition a neutral magistrate for a second warrant.[136] Although images

---

it may be difficult for government to determine what to seize without doing some level of review of everything in the cabinet, as "few people keep documents of their criminal transactions in a folder marked '[crime] records'" (alteration in original) (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir.1990))).

133 Clancy, *supra* note 66, at 208–09 (commenting that a court suggesting the government may not seize or look through a file based on its label is analogous to saying the government may not seize a plastic bag containing a white powder because it is labeled "flour" or "talcum powder" (quoting United States v. Hill, 322 F. Supp. 2d 108, 1090–91 (C.D. Cal. 2004))); *see* United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986) (explaining that "in the age of modern technology and commercial availability of various forms of items, [a] warrant [cannot] be expected to describe with exactitude the precise form the records [might] take" because records of criminal activity—in this case, drugs—might well be found in cassettes, leases, and accounts cards, or in cancelled checks); *see also Carey*, 172 F.3d at 1275 (stating that in cases involving images stored in a computer, the file cabinet analogy may be inadequate because digital and electronic storage is likely to contain a greater variety of information than any previous storage methods).

134 *See* United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) ("Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant."); *see also* Erickson v. Comm'r, 937 F.2d 1548, 1554 (10th Cir. 1991) (finding that drug trafficking activity is often concealed or masked by deceptive records or files); United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) ("There is no way to know what is in a [computer] file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."); United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) ("[H]ackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories."); *Hunter*, 13 F. Supp. 2d at 583 ("Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.").

135 *See infra* Part IV.B (discussing the proper balance between the interests of the government and the individual's Fourth Amendment protections).

136 United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) (noting that by immediately going to a magistrate to obtain a second warrant after discovering the initial image of child pornography, the officer ensured that his search was "reasonable and within the

that are displayed on a computer screen are clearly recognized as within plain view, this approach would not extend the plain view doctrine to closed computer files on a hard drive that are subsequently opened.[137] Nor would this view allow for the seizure of information stored on a network or general server because it would require specified search procedures for sifting through the massive amounts of information, even though the procedures may well fall short in allowing for the discovery of all evidence pertaining to the warrant.[138] This view implicitly suggests that law enforcement officials routinely operate in bad faith and presumes that proactive stipulations are necessary to curb overly zealous law enforcement officials.[139] Ultimately, the special approach is problematic because it severely curtails the ability of officers to conduct general warrants but allows for officers to obtain a second warrant to search the rest of the computer's files regardless.[140]

---

parameters of the [original] search warrant"). This reasoning, however, runs counter to explicitly articulated Supreme Court principles. *See* Arizona v. Hicks, 480 U.S. 321, 327 (1987) (noting "the desirability of sparing police, whose viewing of the object in the course of a lawful search is as legitimate as it would have been in a public place, the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant" when evidence is discovered in plain view). The mere technicality of forcing police to obtain a second warrant does little, if anything, to protect the Fourth Amendment privacy rights of individuals, and creates an undue and unnecessary burden on the part of law enforcement officials. *See id.* at 328.

137 *See Walser*, 275 F.3d at 987 (noting that the individual's Fourth Amendment rights were not violated because the police obtained a second warrant before continuing the search for child pornography files); *Carey*, 172 F.3d at 1275 (employing a subjective intent-based "special approach" that ultimately asks whether the officer searching the computer expected to find the incriminating digital evidence).

138 *See Gray*, 78 F. Supp. 2d at 529 (noting that investigators cannot rely on file suffixes to limit searches for computer files because they do not know if the computer's owner attempted to hide his files by changing the file suffixes—which is both easy and common).

139 *See* United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 (D. Me. Dec. 3, 2009) ("The *CDT* protocols impose extraordinary precautions against police misconduct for all applications for a warrant to search a computer, assuming misconduct will be the rule, not the exception."); *see also* United States v. Kim, 677 F. Supp. 2d 930, 950 (S.D. Tex. Dec. 23, 2009) (finding that "the Government's attempts to claim that they discovered the files while looking for evidence of Computer Intrusion is a clear attempt to justify the government's warrantless search for evidence of child pornography and to manipulate the Court into authorizing their defiance of the Magistrate's order").

140 *See Walser*, 275 F.3d at 987 (holding that because the officer obtained the second warrant to search for files relating to child pornography, he ensured that the "search was reasonable and within the parameters of the [original] search warrant"); *Carey*, 172 F.3d at 1276 (holding that officers should obtain a second warrant in order to continue searching the computer for files relating to child pornography). It further contradicts Supreme Court precedent by restricting the ability of law enforcement to adequately conduct their duties. *See* Dalia v. United States, 441 U.S. 238, 257 (1979) ("[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.").

While implicitly adhering to this special approach, the Ninth Circuit in *Comprehensive Drug Testing* took the judicially unprecedented step of suggesting that the government "forswear reliance" on the plain view doctrine or *any similar doctrine* that would allow the government to retain data it obtained only because it was unable to properly segregate the intermingled evidence.[141] The court reasoned that because the government will ultimately determine the extent of the seizure, which is itself a potentially inaccurate assessment, it will create a powerful incentive to "seize more rather than less."[142] The court further imposed requirements that in future computer evidence cases the government must fairly disclose the *actual* risk of concealment or destruction of evidence as opposed to merely the theoretical risk.[143] Additionally, in what will likely extract significant administrative costs, the court mandated that only specialized computer personnel should sort and separate the seizable and nonseizable data, as denoted in the search warrant.[144]

Demonstrably, courts taking a special approach to the searches and seizures of computer evidence and digital information are unlikely to uphold more general searches of computers or find that the computer's

---

141 *Comprehensive Drug Testing III*, 579 F.3d 998, 998 (9th Cir. 2009) (en banc) (suggesting that in the context of computer evidence cases, "the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine"), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc). *But see Farlow*, 2009 WL 4728690, at 6 (finding that to require the Government to forswear reliance on the plain view doctrine is "an extreme remedy better reserved for the unusual, not common case," and that such a directive "placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair").

142 *Comprehensive Drug Testing III*, 579 F.3d at 998.

143 *Id.* This requirement imposed by the Ninth Circuit is perhaps more properly seen as its attempt to foreclose what it inferred was bad faith on behalf of the government. *See id.* However, in the very same paragraph, the majority opinion recognizes that this bad faith will be adequately dealt with when determining whether to exclude the evidence *vis-à-vis* a motion to dismiss. *See id.* at 999 ("A lack of candor in this or any other aspect of the warrant application shall bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.").

144 *Compare id.* 1000–01, 1006 (finding that "[s]egregation and redaction must be either done by specialized personnel or an independent third party"), *with id.* at 1013 (Callahan & Ikuta, JJ., concurring in part and dissenting in part) (noting that the majority opinion "offers no support for its protocol requiring the segregation of computer data by specialized personnel or an independent third party," and that "this new *ex ante* restriction . . . raises practical, cost-related concerns"). Of significant importance to the concurring judges was the majority's "newly minted search protocol[]" that mandates warrants make clear that "only persons not involved in the investigation may examine and segregate the data." *Id.* at 1011 n.6.

files are subject to the plain view doctrine.[145] Attempting to guard against overbroad warrants that jeopardize the Fourth Amendment rights of innocent Americans as well as criminals, this special approach suggests that applying the plain view doctrine to computer searches gives the government "free rein" to rummage through computers.[146] Proponents further suggest that applying this specialized, more circumscribed approach is easily reconciled with the Supreme Court's precedent in *Hicks*; however, this fails to recognize that unlike the physical property confronted in *Hicks*, digital property and computer evidence create novel opportunities for criminals to disguise or conceal evidence of incriminating character.[147] Ultimately, it appears as though the special approach to computer searches is taking the forefront in the minds of scholars and is beginning to see increased popularity in the judiciary as well.[148]

---

[145] *See Carey*, 172 F.3d at 1273 (finding that because the officers expected to find the subsequent images of child pornography—and therefore did not "inadvertently discover[]" the images—the images could not rightly be considered within plain view). In *Carey*, the defendant argued that the officer's "search of the computers transformed the warrant into a 'general warrant' and resulted in a general and illegal search of the computers and their files." *Id.* at 1271–72; *see also* United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (finding that where a colonel used a personal computer to transport child pornography, the plain view doctrine did not apply to the search of computer files because the warrant did not authorize the search of those files and view was obtained as a result of improper governmental opening, not as a result of seeing what was legitimately in plain view).

[146] *See Comprehensive Drug Testing III*, 579 F.3d at 998 ("If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file—and we have no cavil with this general proposition—then everything the government chooses to seize will, under this theory, automatically come into plain view."); *Carey*, 172 F.3d at 1271–72 (finding that if the government were allowed to use the plain view doctrine it could transform all searches of computers into "general warrant[s]").

[147] *See* Arizona v. Hicks, 480 U.S. 321 (1984) (holding that an officer who moved stereo equipment to see the serial numbers underneath, and who, after subsequently phoning the numbers into headquarters and determining the equipment was stolen, seized the evidence, did not validly do so pursuant to the plain view doctrine). This, however, does not illustrate that the Supreme Court is against invoking the plain view doctrine or even that they are for a more circumscribed reading of it; rather, it merely illustrates that evidence seized pursuant to plain view must be immediately apparent, and that any *search* beyond what is immediately apparent renders the determination of the criminality of the evidence *not immediate*. *See id*. at 324–25.

[148] *See Comprehensive Drug Testing III*, 579 F.3d at 1006 (adopting a special approach to the plain view exception in computer evidence cases, attempting to "update" existing Fourth Amendment jurisprudence to accord computer technology, and ultimately banning government use of the plain view doctrine *or any similar doctrine* in the context of computer evidence cases); *Carey*, 172 F.3d at 1268 (explicitly adopting a special approach to computer evidence cases that relies heavily on the subjective intent or mindset of the investigating officials); Winick, *supra* note 14, at 81 (discussing his version of the "special approach" to computer evidence cases).

C. The Attenuated Closed-Container Analogy

"Container" is a well-defined and highly evolved term within Fourth Amendment jurisprudence.[149] Many courts compare digitally stored data as a form of document and therefore authorize the search of computer files even if the warrant only specifies that writings or records may be searched.[150] This line of reasoning is sympathetic to the varying needs of law enforcement officials and suggests the government need not know the exact "form that records may take."[151] Critics regard this view as overly simplistic because it asserts that there is no distinction between electronic records and physical records.[152] However, this view is consistent with the Supreme Court's precedent in *Andresen v. Maryland* that "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[153] Therefore, under the theory that data is a form of document and the computer is a container holding the

---

[149] *See generally* CLANCY, *supra* note 23, at 40–42 (providing a background as to how containers are treated under the Fourth Amendment); TASLITZ, *supra* note 21, at pt. 1 (providing the same).

[150] *See also* United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (holding that warrant authorizing search for "records" permitted search of "computers, disks, and similar property"); Frasier v. State, 794 N.E.2d 449, 454, 460 (Ind. Ct. App. 2003) (holding that warrant which authorized search of notes and records of marijuana sales also permitted the police to examine computer files).

[151] United States v. Gawryisak, 972 F. Supp. 853, 861 (D.N.J. 1997), *aff'd*, 178 F.3d 1281 (3d Cir. 1999).

[152] United States v. Lievertz, 247 F. Supp. 2d 1052, 1063 (S.D. Ind. 2002). The court in *Lievertz* suggested that there is "no principled distinction between those records kept electronically and those in paper form." *Id.* However, some courts have suggested that this view is sensitive to individuals because there is "no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records." *Hunter*, 13 F. Supp. 2d at 584.

[153] 427 U.S. 463, 482 n.11 (1976); *see Hunter*, 13 F. Supp. 2d at 582, 584 (recognizing the reality that few people store their incriminating records in clearly labeled boxes or containers); *see also* United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) (finding that few people label their belongings that are incriminating with obvious labels); United States v. Gray 78 F. Supp. 2d 524, 528 (E.D. Va. 1999) (suggesting few people label their incriminating evidence in obvious ways). The Supreme Court in *Andresen* observed the following:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.

Andresen, 427 U.S. at 482 n.11.

document, traditional rules of document searches should apply and govern conduct.[154]

Courts—and to a lesser extent scholars—adhering to the container approach to computer evidence have reasoned that there is no need to impute novel approaches into the law each time a novel difficulty arises.[155] Instead, courts have looked to whether the warrant was sufficiently particular to describe the "place[s] to be searched" or the "persons or things to be seized."[156] These courts give deference to the

---

[154] *See, e.g.*, United States v. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998) (explicitly comparing a computer to a closed container and suggesting the application of the law is analogous). In *Barth*, the defendant took his computer to a repair shop and pornographic images of children were subsequently discovered; the computer was searched by police without a warrant. *Id.* at 930. The court found that the defendant did not lose a reasonable expectation to privacy by delivering the hard drive to a computer technician for repairs, so that a warrantless police search of the hard drive violated the Fourth Amendment. *Id.*

More important, however, is the court's reasoning. The court noted that although the protection afforded to a person's computer files and hard drive was not well-defined, it concluded that the Fourth Amendment protection of closed computer files and hard drives was similar to the protection afforded a person's closed containers and closed personal effects. *Id.* at 932. According to the court, outside of automobile searches, a warrant was usually required to search the contents of a closed container because the owner's expectation of privacy related to the contents of that container rather than to the container itself. *Id.* By placing data in files in a storage device such as his hard drive, the court reasoned, the defendant manifested a reasonable expectation of privacy in the contents of those files. *Id.* Further holding that the defendant did not lose his reasonable expectation of privacy in his closed, individual files when he gave the hard drive to the technician, the court stressed that the defendant gave the hard drive to the technician for the limited purpose of repairing a problem unrelated to specific files and also expected that he would have the unit back the following morning to continue his business. *Id.*

[155] *See Comprehensive Drug Testing III*, 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan and Ikuta, JJ., concurring in part and dissenting in part) ("Rather than adopting [a special] efficient but overbroad approach, the prudent course would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication."), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc).

[156] *See* U.S. CONST. Amend. IV; *supra* Parts II.A.1, II.A.2 (discussing how courts have used the warrant requirement and the particularity requirement, respectively, to attempt to reconcile novel difficulties that computers create within the context of the Fourth Amendment). The nature of the crime, for example, might require a broad police search. *See, e.g.*, *Andresen*, 427 U.S. at 480–81 n.10 ("Like a jigsaw puzzle, the whole 'picture' of petitioner's false-pretense scheme . . . could be shown only by placing in the proper place the many pieces of evidence that, taken singly, would show comparatively little."); United States v. Regan, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) ("The degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity investigated."). The type of evidence sought is also relevant; in particular, courts have recognized that documentary evidence may be difficult to describe ex ante with the same particularity as a murder weapon or stolen property. *See, e.g.*, United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("It is true that a warrant authorizing seizure of records of criminal activity permits officers to examine many papers in a suspect's possession to determine if they are within the described category. But allowing some latitude in this

judge who issued the warrant when assessing the sufficiency of the allegations or the description of the items sought.[157] Thus, by allowing the issuing magistrate the ability to set the parameters of the search based on personalized knowledge of the specific facts at hand, courts are able to adequately safeguard Fourth Amendment interests by ensuring warrants are sufficiently particular and supported by probable cause.[158] Much of the disagreement so readily apparent among the courts and academics stems from a conflict over the importance of requiring law enforcement officials to preemptively secure a warrant.[159] Importing

---

regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"); United States v. Zanche, 541 F. Supp. 207, 210 (W.D.N.Y. 1982) ("Unlike other forms of property, business records are often incapable of being itemized one by one, particularly when their existence, but not their precise names or quantity, is all that is known.").

157 *See Comprehensive Drug Testing III*, 579 F.3d at 1012–13 (Callahan, J. and Ikuta, J., concurring in part and dissenting in part) (contending that the majority opinions sweeping guidelines and broad prescriptions "go significantly beyond what is necessary," and that "its protocols are dicta and might be best viewed as a 'best practices' manual").

158 *See supra* Part II.A.1–2 (discussing how courts have used the warrant and the particularity requirements to attempt to reconcile novel difficulties that computers create within the context of the Fourth Amendment).

159 *See* Coolidge v. New Hampshire, 403 U.S. 443, 474 (1971) ("Much the most important part of the conflict that has been so notable in this Court's attempts over a hundred years to develop a coherent body of Fourth Amendment law has been caused by disagreement over the importance of requiring law enforcement officers to secure warrants."). *Compare Comprehensive Drug Testing III*, 579 F.3d at 1000 (holding that in order to guard against future constitutional violations, the issuing judicial officer should insert a preemptive search protocol), United States v. Giberson, 527 F.3d 882, 890–91 (9th Cir. 2008) (holding that where the police did not continue a search until after obtaining an additional search warrant, no constitutional violation occurred), *and In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 959–61 (N.D. Ill. 2004) (holding that a magistrate can condition the search of computers on the government developing a search protocol before the actual search begins in order to prevent a general rummaging of the hard drive and files), *with* United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3 (D. Me. Dec. 3, 2009) ("Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case, and the notion that a busy trial judge is going to be able to invent one out of whole cloth or to understand whether the proposed protocol meets ill-defined technical search standards seems unrealistic."), United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *37 (S.D.N.Y. Apr. 4, 2007) (holding that while a warrant must state with sufficient particularity what is to be seized from a computer, "the warrant need not specify *how* the computers will be searched"), *and* United States v. Maali, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004) (upholding the validity of a search despite the lack of a search protocol in the warrant under the assumption that "[w]hile it may be preferable and advisable to set forth a computer search strategy in a warrant affidavit, failure to do so does not render computer search provisions [unconstitutional]"). *See generally* United States v. Cioffi, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009) (noting that the warrant requirement was meant to act as a "bulwark against the 'general warrant'" that the early colonists so despised); *Vilar*, 2009 U.S. Dist. LEXIS 99409, at *1 (noting that the warrant requirement is the preeminent concern of the Fourth Amendment).

new theories and doctrines as well as imposing stilted judicial guidelines that serve as a beacon for future law enforcement does little to clarify the law surrounding Fourth Amendment searches and seizures involving computer or digital evidence.[160]

Accepting this view, however, does not mean that the wholesale searches of data on computers or computer systems are permitted.[161] Courts instead look to traditional means of limiting the scope of document searches such as the nature of the criminal activity alleged or the nature of the objects sought in the search warrant.[162] Furthermore,

---

[160] *See Comprehensive Drug Testing III*, 579 F.3d at 1013 (Callahan and Ikuta, JJ., concurring in part and dissenting in part) ("A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving. Accordingly, I cannot join in the majority's approach regarding application of the plain view doctrine to digital evidence cases."); *see also id.* at 1015, 1017 (Bea, J., concurring in part and dissenting in part) (agreeing with "the majority's analysis of the issues presented in this case, *as applied to this case only*" and adding that "[s]uch a rule departs from existing Supreme Court precedent regarding the 'plain view' exception . . . and [does] so *without a single citation* to the Supreme Court's extensive precedent on the subject" (emphasis added)).

[161] *See* People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (holding that police "may search the location authorized by the warrant, including any containers at that location that are reasonably likely to contain items described in the warrant", that "[t]his container rationale is equally applicable to nontraditional, technological 'containers' that are reasonably likely to hold information in less tangible forms," and that courts cannot expect search warrants "to anticipate every form an item or repository of information may take, and therefore courts have affirmed the seizure of things that are similar to, or the 'functional equivalent' of, items enumerated in a warrant, as well as containers in which they are reasonably likely to be found"). This is not to say, however, that courts adopting this view underestimate the differences in physical and digital evidence and documents; rather, they merely give significantly less weight to these differences or view them as immaterial to the analysis. *See id.* (applying the container theory despite recognizing a heightened degree of intermingling of relevant and irrelevant evidence); *see also* United States v. Hunter, 13 F. Supp. 2d 574, 581, 583–84 (D. Vt. 1998) (addressing the concerns of the intermingling of relevant and irrelevant information).

[162] *See, e.g.*, *Comprehensive Drug Testing II*, 513 F.3d 1085, 1111–12 (9th Cir. 2008) (disagreeing with the dissent that the government should be forced to rely on the target of the search to point out the relevant files and copy only specific folders), *vacated*, 545 F.3d 1106 (9th Cir. 2008), *decision reached on appeal*, 579 F.3d 989 (9th Cir. 2009). The first panel decision of *Comprehensive Drug Testing* aptly recognized the following:

> "The government should not be required to trust the suspect's self-labeling when executing a warrant." Agents had no duty to rely on CDT personnel to point out the files seizable under the warrant. Like most searched parties, CDT had an incentive to avoid giving over documents of which the government might be unaware and to read the search warrant as narrowly as possible. Moreover, the government had no reason to confine its search to "key words" such as the names of the baseball players. "Computer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery

because this view permits the law enforcement need to adapt with the various circumstances, it allows for a more proper administration of justice.[163]

Finally, advocates of the container analogy—or perhaps more generally those opposing the special approach and opting for a more traditional case-by-case analysis—argue that the establishment of guidelines stands directly against the common law method of reasoned decisionmaking.[164] In a time when computer technology is evolving at a tremendous pace, creating concrete guidelines that firmly establish bright lines is arguably unseemly.[165] By evaluating each case on its own merits and attempting to resolve no more than is necessary, courts can employ the traditional common law method, which "recognizes the limitations of human ingenuity and wisdom."[166] The common law

---

> simply because of [the defendants'] labeling of the files." Such a limited search could easily have overlooked documents crucial to the investigation, such as the specimens at Quest, which were identified only by number.

Id. (citations omitted).

[163] *See Comprehensive Drug Testing III*, 579 F.3d at 1018 (Bea, J., concurring and dissenting) (noting that "the establishment of guidelines . . . goes against the grain of the common law method of reasoned decisionmaking, by which rules evolve from cases over time," and that "[b]y focusing on the 'plain view' exception as applied to [the case at bar] . . . we would be employing the traditional common law method of deciding novel questions of law," and that this method "recognizes the limitations of human ingenuity and wisdom, by limiting [judicial] decisions as precisely as possible to the case at hand"). Circuit Judge Bea aptly recognizes in his dissent that "[t]he common law method permits us to evaluate different cases over time to discern the most sensible rule given the technologies that develop." *Id.*

[164] *Id.* To some extent, the Tenth Circuit—itself explicitly adopting a special approach to computer evidence—has chosen to adhere to the common law method of reasoned decisionmaking based narrowly on the facts at hand, such as noting that

> [t]he essential inquiry when faced with challenges under the Fourth Amendment is whether the search or seizure was reasonable—reasonableness is analyzed in light of what was reasonable at the time of the Fourth Amendment's adoption. It is axiomatic that the Fourth Amendment was adopted as a direct response to the evils of the general warrants in England and the writs of assistance in the Colonies.

O'Rourke v. City of Norman, 875 F.2d 1465, 1472 (10th Cir. 1989) (citations omitted).

[165] *See Comprehensive Drug Testing III*, 579 F.3d at 1018 (noting that the establishment of guidelines "is particularly troublesome in a rapidly developing area of law such as this one, as computer search capabilities improve exponentially by the month"). Circuit Judge Bea also noted that the courts do not have the same competitive advantage that Congress has for establishing guidelines, perhaps implicitly suggesting that turning to the legislature is one avenue for dealing with such a timely dilemma. *See id.*

[166] *Id.* The primary reason for Judge Bea's dissent was the fact that by issuing bright-line, prophylactic rules, the majority opinion "short-circuits this process in an area where the capabilities of computer software are still rapidly evolving." *Id.* Furthermore, although both the Tenth Circuit and Ninth Circuit seemingly employ similar strategies in combating

method permits courts to evaluate different cases over time to determine the most sensible rule at any given moment and given any new technologies that may develop.[167]

All in all, the different approaches to applying the plain view exception attempt to reconcile the needs of adequate law enforcement on the one hand, with the expectations of privacy that are guaranteed to us through the devices of the Fourth Amendment, on the other hand.[168] Although these are indeed noble causes and should be considered in proper Fourth Amendment analysis, the current approaches to this novel difficulty fail to safeguard the interests of both parties involved.[169] The special approaches attempting to deal with this problem strongly favor the individual and ultimately cripple the ability of officials to enforce the law.[170] Advocates of the closed-container analogy fail to sufficiently defend the constitutional rights provided by the Fourth Amendment while attempting to apply traditional values and concepts implicit in Fourth Amendment jurisprudence.[171] It is inevitable that the Supreme Court will consider the issue, and when it does, it should employ an approach that adequately balances each of the competing interests

---

the plain view doctrine, the majority's issuance of bright-line rules contradicts the special approach of the Tenth Circuit. *See id*. at 1018 n.3 (noting that the majority's broad, prophylactic guidelines "conflict with the more cautious, common law-style approach of the Tenth Circuit, which has implicitly recognized the 'plain view' exception exists in [this] context . . . but has not delineated its precise scope").

167 *Id*. at 1018. Interestingly, Judge Bea actually contends that the majority opinion in *Comprehensive Drug Testing* conflicts with the Tenth Circuit's opinion in *Carey*, at least insofar as it attempts to establish concrete judicial guidelines. *See id.* It seems clear that some of the *Comprehensive Drug Testing* opinion conflicts with *Carey*, because *Carey* implicitly recognized that the plain view exception *applies* in computer evidence cases, whereas *Comprehensive Drug Testing* explicitly contends that the plain view exception *should not* apply. *Id*. at 998. *Compare Comprehensive Drug Testing III*, 579 F.3d at 998 (majority opinion) (holding that "the government should . . . forswear use of the plain view doctrine *or any similar doctrine*" (emphasis added)), *with* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (holding that satisfaction of the plain view exception to the warrant requirement should ultimately turn on the subjective intent of the searching officials). *See also* United States v. Giberson, 527 F.3d 882, 890–91 (9th Cir. 2008) (holding that no constitutional violation occurred where the government inadvertently discovered child pornography and subsequently applied for an additional warrant).

168 *See supra* Part III (discussing the different approaches courts have created to reconcile the competing interests in this area).

169 *See supra* Part III (analyzing the different approaches that courts have taken and suggesting that each of them fails to adequately weigh and balance the competing interests).

170 *See supra* Part III.B (evaluating the special approaches to the plain view doctrine as applied to computer evidence).

171 *See supra* Part III.C (analyzing the closed-container approach that a series of courts have taken to attempt to apply Fourth Amendment values to novel difficulties that arise in the context of computer-based evidence).

involved and mandate a course of action that appropriately safeguards each of the various concerns.[172]

IV. CONTRIBUTION

Every government search or seizure of a digital, electronic, or computer-related device poses a potential problem for law enforcement officials.[173] This Part proposes a solution that is sensitive to these concerns while still protecting individual liberties.[174] Some have argued that in order for Fourth Amendment jurisprudence to remain consistent, courts should analyze the problems on a case-by-case basis, offering little, if any, by means of prophylactic advice.[175] Others have determined that current Fourth Amendment principles are simply insufficient to handle such technological advances and that a new, more specialized body of law must emerge to efficiently handle these complex new problems.[176] Nonetheless, all are in favor of a solution that adequately balances the interests of law enforcement officials in carrying out their duties and responsibilities with the privacy, possessory, and constitutional interests to which every American is entitled.[177] This Note espouses such a solution by implementing the inadvertent discovery requirement for plain view seizures that grants latitude to law enforcement while preventing general and pretextual searches. Additionally, this Note outlines the proposed solution's rationale and practical application.[178] Accordingly, the Supreme Court should

---

172 *See infra* Part IV (proposing a workable solution to this problem).

173 *See supra* Part II.B.1 (discussing the novel difficulties that digital, electronic, and computer evidence creates); *supra* Part III.A–B (discussing and analyzing the differing approaches that courts have taken to attempt to solve these complex problems).

174 *See infra* Part IV.A (proposing that the Supreme Court should implement the inadvertent discovery requirement for valid plain view seizures of electronically stored and computer-related evidence).

175 *See, e.g.*, *supra* note 163 (discussing the inherent advantages to narrowing the holding to what is essential and allowing the law to develop slowly but surely as a principle of the common law).

176 *See, e.g.*, *supra* note 148 (discussing different attempts to "update" Fourth Amendment jurisprudence and create new standards and tests of substantive law).

177 *See, e.g.*, *supra* Part III.B–C (providing that those in favor of the "special approaches" and those in favor of using analogies attempt to balance the competing interest of law enforcement and individual citizens).

178 *See infra* Part IV.B.1 (discussing the rationale behind implementing or retaining the inadvertent discovery requirement for plain view seizures); *infra* Part IV.B.2 (applying the proposed standard to the facts of *Comprehensive Drug Testing*). Further, whether this proposal is termed "retention" or "implementation" is irrelevant to the inquiry at hand. What is paramount is whether the discovery of evidence that is not inadvertent will render the plain view doctrine inapplicable to justify the seizure of the evidence, notwithstanding whether the requirement is "retained" or "implemented."

confront the issue directly, despite its controversial nature, because allowing the law to remain so staunchly unsettled compromises the interests of millions of Americans.[179]

The Supreme Court should grant certiorari to a case factually similar to *Comprehensive Drug Testing*—a case requiring direct application of the plain view doctrine to computer-related evidence. The Supreme Court should apply existing Fourth Amendment plain view principles while preventing the most prominent evil of the Fourth Amendment—the general warrant.[180] The Court should remain cognizant that vast differences exist between physical evidence and digital evidence.[181] Upon recognizing this distinction, the Court could either: (1) overrule *Horton* explicitly and reinstate the inadvertent discovery requirement entirely; or (2) distinguish the case from *Horton*.[182] However, because complete reinstatement of the inadvertent discovery requirement would require the Court to overrule a litany of cases that have further developed plain view jurisprudence and is ultimately unnecessary, the most prudent course of action is distinguishing between physical and digital evidence.[183]

---

[179] *See* Brief for the United States in Support of Rehearing En Banc by the Full Court, *Comprehensive Drug Testing III*, 579 F.3d 989 (2009) (No. 05-10067) (suggesting that police and courts alike are not sure to what extent the judicially crafted guidelines are mandatory or whether they should apply to other types of evidence such as cellular phones or similar devices).

[180] *Cf.* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The manifest purpose of this particularity requirement was to prevent general searches," and that "the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit").

[181] *See supra* Part II.B.1 (discussing the novel difficulties created by inherent differences between physical and electronic evidence); *supra* Part III.A (discussing the circumstances under which searches and seizures of electronic information are most likely to become general and exploratory in nature—and therefore unconstitutional).

[182] *See supra* notes 52–54, 61–62 (discussing the *Coolidge* and *Horton* decisions and the Court's decision to remove the inadvertent discovery requirement from plain view analysis).

[183] Overruling *Horton* would allow the court to reinstate the inadvertent discovery requirement of the plain view doctrine, but would reinstate the requirement for *all* plain view seizures. The Court in *Horton* disposed of the inadvertent discovery requirement but never mentioned the differences in physical and digital evidence. *See* Horton v. California, 496 U.S. 128, 129–30 (1990), (suggesting the inadvertent discovery requirement is not necessary as applied to a car on the defendant's property). *Horton* dealt entirely with physical evidence, however. *Id.* It is markedly undisputed that the risk of general warrants and government overreaching is far greater when dealing with computer-related evidence. *See Comprehensive Drug Testing III*, 579 F.3d 989, 1004 (9th Cir. 2009) (en banc) (finding that "[t]his pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant" and accepting "the reality that such over-seizing is an inherent part of the electronic search process"), *revised and superseded per curiam*, 621

A. Proposed Solution: Retain the Inadvertent Discovery Requirement for Electronically Stored Evidence

Stare decisis concerns counsel that complete abrogation of the *Horton* reasoning is unnecessary. When faced with physical evidence, the inadvertent discovery requirement may actually remain unnecessary largely because objective criteria effectively limit the scope of a seizure. This is not so with digital evidence. Objective characteristics such as size limit the scope of a physical search. For instance, police cannot search for stolen stereo equipment in small dresser drawers, a vehicle inside of a home (except the garage), or, perhaps more illustratively, an entire building because contraband is found in one container.[184] Thus, the objective characteristics of physical evidence help determine the scope of the search or seizure—the scope is defined by "the object of the search and the places in which there is probable cause to believe the object may be found."[185] However, because an officer cannot know the contents of a computer file until it has already been opened, these characteristics cannot adequately guide police seizures or limit intrusions upon constitutional liberties.[186] Thus, although requiring inadvertent discovery may not be necessary to limit plain view seizures of physical evidence, the same cannot rightly be said of electronically stored

---

F.3d 1162 (9th Cir. 2010) (en banc); *see also* Kerr, *supra* note 65, at 280, 289–90 (suggesting that physical world rules impose practically no limitations on searches of computer evidence and "permit extraordinarily invasive government powers to go unregulated"); Winick, *supra* note 14, at 80 (suggesting adamantly that general searches are far more prevalent in the context of computer-related evidence); *supra* Part II.B (discussing the difficulties of preventing general searches); *supra* Part III.A (analyzing the circumstances under which searches are more likely to become general or exploratory in nature). Nonetheless, because overruling *Horton* would undo and overturn much of the twenty years of case law that have developed since its inception and because physical evidence creates fewer problems than electronically stored evidence, overruling *Horton* is perhaps unwarranted.

184 *See* United States v. Ross, 456 U.S. 798, 824 (1982) ("Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.").

185 *Horton*, 496 U.S. at 140–41 ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." (quoting *Ross*, 456 U.S. at 824)). Assuming, *arguendo*, that this notion does adequately protect the constitutional interests of citizens by guiding the efforts of law enforcement, such objective criteria are inherently absent when courts are confronted with computer-related evidence. *See Comprehensive Drug Testing III*, 579 F.3d at 1004 (recognizing that law enforcement cannot know the contents of a file or determine its relevancy to the search until the file has been opened and examined); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (emphasizing the same).

186 *See Comprehensive Drug Testing III*, 579 U.S. at 1004 ("There is no way to be sure exactly what an electronic file contains without somehow examining its contents . . . .").

evidence.[187] Allowing such warrantless seizures condones grave erosions to personal liberties.

The Supreme Court should therefore declare that *Horton*'s alteration of the plain view doctrine is inapplicable to computer-related evidence. The Court should announce that the plain view doctrine, as applied to computer-related evidence, is consistent with the view of Justice Stewart's opinion in *Coolidge* and Justice Brennan's dissent in *Horton* by ruling that

> *as applied to electronically stored and computer-related evidence, the final limitation on the application of the plain view doctrine is that the discovery of evidence in plain view must be inadvertent.*[188]

B. Commentary

This requirement is necessary to ensure that initially valid—and therefore limited—seizures do not become general. Where the discovery of evidence is anticipated—that is, where police know in advance the location of the evidence and intend to seize it—requiring that officials obtain a warrant imposes no cognizable inconvenience in a system that regards warrantless searches as per se unreasonable. This rule does not create a cost on efficient law enforcement; it is the Fourth Amendment itself that imposes such limits on government officials. The inadvertent discovery requirement is merely the attendant manifestation of the Fourth Amendment's own requirement that the items to be seized be particularly described in a warrant. Police may not intentionally search for and seize items not described therein. Where the government wishes to invoke the plain view doctrine, it must show that no probable cause for the seizure existed at the time that the particular warrant was issued. This requirement is nothing more than a restatement of the explicit

---

[187] According to Justices Stewart, Brennan, and Marshall, the inadvertent discovery requirement is not actually a judicially crafted notion but rather it is a necessary incident of the Fourth Amendment's explicit mandates. *See, e.g.*, *Horton*, 496 U.S. at 142 (Brennan and Marshall, JJ., dissenting) ("In eschewing the inadvertent discovery requirement, the majority ignores the Fourth Amendment's express command that warrants particularly describe not only the *places* to be searched, but also the *things* to be seized."); Coolidge v. New Hampshire, 403 U.S. 443, 468 (1971) ("The limits on the doctrine are implicit in the statement of its rationale.").

[188] The italicized text is the original contribution of the author and is modeled after both the language and notion of Justice Stewart's plurality opinion in *Coolidge* and Justice Brennan's dissenting opinion in *Horton*. *Cf. Horton*, 496 U.S. at 142 (Brennan, J., dissenting) ("I remain convinced that Justice Stewart correctly articulated the plain-view doctrine in [*Coolidge*]."); *Coolidge*, 403 U.S. at 469 ("The second limitation [on application of the plain view doctrine] is that the discovery of evidence in plain view must be inadvertent.").

mandate of the Fourth Amendment's particularity requirement. It is but a logical extension of the notion, heralded by the Court in *Horton*, that all warrantless searches and seizures are unreasonable absent exigent circumstances.[189]

1. The Rationale

The plain view exception to the warrant requirement primarily operates to supplement the efforts of law enforcement officials by allowing warrantless seizures where "the inconvenience [of procuring a warrant] incurred by police is simply not that significant."[190] However, where the discovery of the evidence is expected, the justification of inconvenience is entirely baseless. The few exceptions to the warrant requirement provide for those cases where the societal costs of obtaining a warrant, such as danger to law enforcement officers or the risk of destruction of evidence, outweigh the reasons for prior recourse to a neutral and detached magistrate. Because, however, each exception to the warrant requirement invariably impinges on the protective purposes of the Fourth Amendment, the exceptions have been carefully delineated and the burden remains on those seeking to enforce the exception to show its necessity. Without the inadvertence requirement in plain view analysis of electronically stored information, the Fourth Amendment's goals of encouraging police resort to the warrant process and limiting authorized intrusions to the smallest extent possible is substantially and irreparably subverted.

Although requiring inadvertent discovery may appear insensitive to the efforts of law enforcement officials, this is a misconception. The Fourth Amendment does not deny law enforcement officials "the support of the usual inferences which reasonable men draw from evidence."[191] The Fourth Amendment merely requires that these inferences be drawn by neutral and detached magistrates. Further, this requirement remains necessary to prevent pretextual seizures of electronic information because there is no rationale to excuse officials from the warrant requirement when they know the location of evidence, have probable cause to seize it, intend to seize it, and yet fail—willfully or neglectfully—to obtain a warrant particularly describing it. The inadvertence requirement makes planned searches and seizures without a warrant impossible. A rule allowing seizures of items not listed on a

---

189 *See Horton*, 496 U.S. 128 (reinforcing the notion that warrantless searches are per se unreasonable absent exigent circumstances).

190 Steagald v. United States, 451 U.S. 204, 222 (1981).

191 Johnson v. United States, 333 U.S. 10, 13–14 (1948).

warrant and not inadvertently found would wholly abrogate the particularity and warrant requirements of the Fourth Amendment.

If law enforcement officials abide by the explicit commands of the Fourth Amendment, they should have no reason to spite this requirement. In fact, there should be no additional burden upon law enforcement officials whatsoever. The Fourth Amendment protects citizens' privacy and possessory interests by mandating that a neutral and detached magistrate issue the warrant. The interests of law enforcement officials in expedient investigation are de minimis when balanced against these possessory and privacy interests explicitly protected by the Constitution.

Where there exists no justification for excusing the warrantless seizure, doing so would violate the constitutional requirement that warrants particularly describe the things to be seized and that neutral and detached magistrates make probable cause determinations. It would ultimately "fly in the face of the basic rule that no amount of probable cause can justify a warrantless seizure."[192] Without a showing that law enforcement efforts are impeded or the administration of justice is hindered, there exists no conceivable rational basis for allowing the warrantless seizure of electronically stored information discovered intentionally. Where government officials are present to execute a warrant and seize items not particularly described, it must be shown that the officers had no intention of searching for and seizing those items. Inconvenience to the police and a slight delay caused by preparing papers for a magistrate are never convincing reasons to bypass the warrant requirement.[193] The warrant requirement of the Fourth Amendment is not some mere technicality or inconvenience; it is an explicit command of the Constitution.[194] Accordingly, the police may not—consistent with the Constitution and traditional Fourth Amendment values—plan a plain view seizure.[195]

Ultimately, the sensitivity and import of the interests presented when constitutional freedoms clash with law enforcement efforts leave

---

192 *Coolidge*, 403 U.S. at 471.

193 Trupiano v. United States, 334 U.S. 699, 706 (1948).

194 *Keith*, 407 U.S. 297, 315 (1972) ("The warrant clause of the Fourth Amendment is not dead language."). The Court also noted that the Fourth Amendment, and the warrant requirement in particular, should remain "'an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a party of any system of law enforcement.'" *Id*. at 316 (quoting *Coolidge*, 403 U.S. at 468).

195 Horton v. California, 496 U.S. 128, 144 (1990) ("A decision to invade a possessory interest in property is too important to be left to the discretion of zealous officers 'engaged in the often competitive enterprise of ferreting out crime.'" (quoting *Johnson*, 333 U.S. at 14)).

attorneys relying on limited principles that sweep no more broadly than appropriate in the context of a particular case. Unequivocal retention of the inadvertent discovery requirement provides an equitable boundary between the competing interests involved with seizures of electronically stored evidence. It recognizes the strength of the legitimate state interest in allowing police wide latitude in conducting comprehensive investigations, yet also shields the individual from overt government intrusion upon basic constitutional liberties. Notwithstanding the strength of the State's interest, the government may not, consistent with the Fourth Amendment, know in advance the location of certain evidence and intend to seize it, relying on the plain view doctrine solely as a pretext.

2. Practical Application

Maintaining the inadvertent discovery requirement for plain view seizures of electronically stored information should ultimately affect very few cases. It remains necessary, however, to ensure that government searches do not become general and exploratory in nature. For example, in the situation involving a search of a home computer for business or personal records of a specific crime, if the government officials inadvertently open a file that contains child pornography, the government would still be able to seize the information and use it at a later date. This is because the discovery of the evidence was inadvertent. By contrast, if the government knew ahead of time of the child pornography and had an intention to seize it, mandating that they obtain a warrant creates no additional obstacle or inconvenience. Thus, requiring that the discovery of evidence be inadvertent ensures that officials do not obtain the child pornography under false pretenses or without a warrant particularly describing the items to be seized. This rule is sensitive to law enforcement interests in conducting expedient investigations by allowing warrantless seizures when contraband is inadvertently discovered, as well as to the Fourth Amendment's explicit commands regarding particularized warrants and probable cause determinations.

To further illustrate the application of this concept, an application to the facts of *Comprehensive Drug Testing* is illustrative.[196] Instead of proscribing the government's use of the plain view doctrine entirely, the Court should examine whether the seizure complied with the four

[196] *See Comprehensive Drug Testing III*, 579 F.3d 989 (9th Cir. 2009) (en banc), *revised and superseded per curiam*, 621 F.3d 1162 (9th Cir. 2010) (en banc).

elements of a valid plain view seizure.[197] The analysis would follow that (1) the evidence was in plain view; (2) the investigators were in a lawful position because they had a warrant to search for information pertaining to the ten specified players; and (3) the incriminating nature of the evidence was immediately apparent because it was precisely the same evidence as what allowed them the initial search and seizure.[198] However, the fourth and final element is not satisfied because the law enforcement officials knew the location of the evidence ahead of time, intended to seize it, and failed to procure a warrant—either through neglect or lack of probable cause; the discovery of the evidence cannot rightly be classified "inadvertent" and the government must return the seized information.[199] Because the government did not discover the evidence inadvertently, it did not satisfy all of the requisite elements of a plain view seizure and the seizure was unconstitutional.[200]

The government in *Comprehensive Drug Testing* was fully aware of the location of the information relating to the other professional athletes.[201] In fact, after obtaining nearly all of the information contained in the search warrant, the government "peruse[d]" the rest of the directory in an attempt to collect as much incriminating information as possible.[202] It is precisely this type of governmental overreaching that warrants the implementation or retention of the inadvertent discovery requirement in the context of electronically stored evidence. Without such a requirement, well-intentioned but often zealous law enforcement officials would smother the constitutional rights of the citizenry.[203]

---

197 The four elements of valid plain view seizures of electronically stored evidence, as proposed by this Note are that (1) the evidence must be in plain view, (2) the officer must view the evidence from a lawful vantage point, (3) the illegality of the evidence must be immediately apparent, and (4) the discovery of the evidence must be inadvertent. *See supra* notes 54 & 61 (discussing the elements of the plain view doctrine as articulated in *Coolidge*, and how the inadvertent discovery requirement was subsequently trimmed from the requisite inquiry by the majority decision in *Horton*). Perhaps *Horton* might best be understood to modify *Coolidge* only insofar as it applies to physical evidence. Because the Court was not confronted with electronically stored evidence, the Court did not have to decide that issue. *See Horton*, 496 U.S. at 140–42 (discussing specifically the tangible characteristics of physical evidence that render the inadvertent discovery requirement arguably superfluous). Thus, this Note offers a guide as to what the Court should do when it confronts the issue at last.

198 *But cf. Comprehensive Drug Testing III*, 579 F.3d at 1005 (mandating that the government forswear use of the plain view doctrine or any similar doctrine).

199 *Id.* at 999–1000.

200 *Id.* at 997–99.

201 *Id.* at 999.

202 *Id.* at 999–1000.

203 *See* Horton v. California, 496 U.S. 128, 143–47 (1990) (Brennan, and Marshall, JJ. dissenting) (arguing that even as applied to physical evidence, the inadvertent discovery

To equate patently warrantless seizures of electronically stored information with valid plain view seizures demeans the grand conception of the Fourth Amendment and its lofty purpose in the historic struggle for freedom.[204] The plain view exception to the warrant requirement is a necessary incident of legitimate law enforcement efforts, but the intentional seizure of items not particularly described is altogether different.[205] Although the interests of the state are by no means trivial or insignificant, they compel the conclusion that these interests cannot justify the substantial damage and erosion to constitutional rights that inevitably result from whimsically allowing warrantless seizures of electronically stored information.[206]

V. CONCLUSION

Two of the most reinforced rules of the Fourth Amendment are that warrantless searches are per se unreasonable and warrants must be sufficiently particularized. From these two fundamental principles flows the assumption that police cannot seize evidence without a warrant merely because they position themselves in a way that makes the evidence visible. Cognizant of this, the Court in *Coolidge* articulated a standard for plain view seizures when faced with physical evidence, which the Court previously found unnecessary in *Horton*.[207] However,

---

requirement is necessary to keep law enforcement officials from eroding and intruding upon basic constitutional liberties).

[204] *Cf. Keith*, 407 U.S. 297, 318 (1972) ("Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." (citing Beck v. Ohio, 379 U.S. 89, 96 (1964))); Marcus v. Search Warrant, 367 U.S. 717, 724 (1961) ("Historically the struggle for freedom . . . in England was bound up with the issue of the scope of the search and seizure power.").

[205] *See Horton*, 496 U.S. at 144–45 (finding that absent exigent circumstances there is no reason to allow warrantless seizures because "[t]he rationale behind the inadvertent discovery requirement is simply that we will not excuse officers from the general requirement of a warrant . . . if the officers know the location of evidence, have probable cause to seize it, intend to seize it, and yet do not bother to obtain a warrant particularly describing that evidence").

[206] *See id.* at 144 (citations omitted) ("A decision to invade a possessory interest in property is too important to be left to the discretion of zealous officers 'engaged in the often competitive enterprise of ferreting out crime.'" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))); *see also* United States v. Rabinowitz, 339 U.S. 56, 68 (1950) ("The framers of the Fourth Amendment must have concluded that reasonably strict search and seizure requirements were not too costly a price to pay for protection against the dangers incident to invasion of private premises and papers by officers, some of whom might be overzealous and oppressive.").

[207] *See supra* notes 54 & 61 (discussing the original four elements of valid plain view seizures as articulated in *Coolidge* and the subsequent revision of the doctrine in *Horton* that saw the tailoring of the inadvertent discovery requirement).

considering the Court has always been wary of the "grave dangers" inherent in authorizing a seizure of a person's papers that are not inherent in physical evidence searches—and has yet to consider the Fourth Amendment's application to electronically stored information—it is likely the Court will find the vast differences between physical and digital evidence significant.[208]

As exemplified by *Comprehensive Drug Testing* and similar cases, law enforcement officials are often involved in the competitive enterprise of "ferreting out crime" and are therefore occasioned to overzealous tendencies. The occurrence of such evils increases greatly in the context of electronically stored information. Requiring inadvertent discovery should not at all hinder the efforts of law enforcement officials to obtain the evidence necessary for conviction of crimes to which they have probable cause. Nonetheless, this requirement remains necessary to ensure that when the plain view doctrine is applied in the context of electronically stored evidence, it complies with the text of the Fourth Amendment. By permitting this exception to the warrant requirement, courts are tolerating government officials' direct violation of the Fourth Amendment. Therefore, exceptions must be drawn as narrowly as possible. It cannot be said with enough emphasis that "[i]t is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon."[209]

It is plausible that maintaining the inadvertent discovery requirement for plain view seizures of electronically stored evidence will affect relatively few police seizures. However, as Justice Bradley wisely observed over a century ago, "illegitimate and unconstitutional practices get their first footing . . . by silent approaches and slight deviations from legal modes of procedure."[210] With this concern in mind, the Supreme Court must establish a standard that adequately protects the privacy and possessory interests of the individual while accommodating law enforcement's legitimate need for flexibility in conducting computer searches. Implementing or retaining the inadvertent discovery requirement in the context of plain view seizures of electronically stored evidence offers the most viable method for ensuring that government seizures of electronically stored evidence do not become general or exploratory and comply with the explicit commands of the Fourth

---

208 *Cf.* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects.").

209 Boyd v. United States, 116 U.S. 616, 635 (1886).

210 *Id.*

Amendment. This standard will neither unduly burden the efforts of law enforcement authorities to maintain order in a civilized society nor authorize unrestrained intrusions upon the privacy of the American citizenry.

Nicholas Hood[*]

[*] J.D. Candidate, Valparaiso University School of Law (2011); B.S., Economics and Marketing, Summa Cum Laude, Missouri Valley College (2008). I would first like to thank my parents for their unconditional love and support in all that I endeavor to accomplish, for their candid criticisms when I have inevitably lost my way, and for teaching me the value of hard-work, faith, and dedication. To my father, Rickard W. Hood, the greatest attorney and most intelligent man I have to this point had the privilege of knowing, for teaching me what it means to be a truly good person and instilling within me unrelenting self-confidence and perseverance. And to my mother, Pamela K. Hood, who, with the most sincere and selfless heart, has devoted her life to her children's well-being and who I strive to be like more and more each day. I would further like to thank my siblings, Chad, Grant, and Cassie, who bore the brunt of my sarcasm and antagonism along the way and did so with unsurpassed good-humor and grace. Finally, a special and heartfelt thanks to my friends and family more generally, of whom there are too many to specifically name herein, who have remained by my side through thick and thin, who make the life I lead worth living, and who have helped me remain sane and grounded through this three-year tussle we call "law school."